Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 524038, 22 pages
http://dx.doi.org/10.1155/2015/524038

Review Article

A Review of Secure Routing Approaches for Current and Next-Generation Wireless Multimedia Sensor Networks

Mohammed Abazeed,[1] Kashif Saleem,[2] Abdelouahid Derhab,[2] Mehmet A. Orgun,[3] Norsheila Fisal,[1] Jalal Al-Muhtadi,[2,4] and Suleiman Zubair[1]

[1]*Faculty of Electrical Engineering, Universiti Teknologi Malaysia, 81310 Johor Bahru, Johor Darul Ta'zim, Malaysia*
[2]*Center of Excellence in Information Assurance (CoEIA), King Saud University (KSU), Riyadh 11451, Saudi Arabia*
[3]*Intelligent Systems Group (ISG), Department of Computing, Macquarie University, NSW 2109, Australia*
[4]*College of Computer and Information Sciences (CCIS), King Saud University (KSU), Riyadh 11451, Saudi Arabia*

Correspondence should be addressed to Mohammed Abazeed; mohmbaz@gmail.com

Received 27 January 2015; Revised 4 June 2015; Accepted 8 June 2015

Academic Editor: Sana Ullah

Multimedia applications are gradually becoming an essential—and flourishing—part of our daily lives. The area of wireless sensor networks is not an exception to this trend, as multimedia data have attracted the attention of researchers. Their importance is due to the shift of focus from traditional scalar sensors to sensors equipped with multimedia devices, as well as to the next-generation wireless multimedia sensor networks (WMSNs). The highly sensitive nature of multimedia traffic makes data routing with security even more important in WMSNs. This paper discusses the challenges of secure routing in WMSNs, where most of the proposed works in the literature deal with routing and security as individual issues. A critical and comprehensive review of state-of-the-art routing and security approaches for WMSNs is presented, followed by the discussion of their limitations and features. It is hoped that this extensive review and discussion ultimately identifies the future research directions and the open challenges of secure routing approaches in WMSNs.

1. Introduction

Wireless multimedia sensor networks (WMSNs) are a newly developed type of wireless sensor networks (WSNs), in which the wireless sensor nodes are equipped with cameras, microphones, and other sensors that generate multimedia data. The development of the WMSNs has been the result of progress in the complementary metal-oxide-semiconductor (CMOS) technology, which has led to the development of single-chip camera modules that could be easily integrated into sensor nodes [1]. This integration between multimedia sources and cheap communication devices motivates the research on WMSNs. WMSNs enhance existing WSN applications and enable a new and broad range of applications, like multimedia surveillance, traffic management, automated assistance, environmental monitoring, and industrial process control. WMSNs have additional features and requirements compared to WSNs, such as high bandwidth demand, bounded delay, acceptable jitter, and a low packet loss ratio.

These characteristics impose more strains on the already resource-constrained devices in terms of energy consumption, memory, buffer size, bandwidth, and processing capabilities [2]. Meeting the quality of service (QoS) requirements for multimedia data within the aforementioned constraints is a significant challenge. Routing protocols designed for WSMNs must consider the requirements and the resource-constrained nature of WMSNs to meet the QoS requirements. Table 1 summarizes the differences between WSNs and WMSNs.

In recent years, the concept of next-generation wireless sensor networks has emerged. These networks aim to bring about a paradigm shift to future application scenarios. In future surveillance systems, a set of mobile multimedia sensor motes equipped with high resolution cameras will be capable

Table 1: Difference between WSNs and WMSNs.

	WSN	WMSN
Applications	Monitoring a variety of physical parameters, habitat monitoring, air or water quality monitoring, hazard monitoring, disaster monitoring	Multimedia surveillance, traffic avoidance, enforcement, and control, environmental monitoring, industrial process control
Architecture	Flat architecture, hierarchical architecture	Single-tier flat, single-tier clustered, multitier
Design challenges	Limited energy capacity, limited hardware resources, massive and random deployment, dynamic and unreliable environment	Multimedia source coding, high bandwidth demand, application-specific QoS requirements, multimedia in-network processing, energy consumption, coverage, resource constraints, variable channel capacity, context-aware sensing, interconnection with other networks
Hardware	Augmented general-purpose personal computers (PCs), dedicated sensor nodes, and system-on-chip (SoC) sensor nodes	Audio sensors, low-resolution sensors, medium-resolution video sensors
Security	Application dependent	
QoS	Application dependent	Very important
Privacy	Needed	Important as the multimedia content might reveal the sender's identity or location

Table 2: The possible attack types in the network layer [3].

Layer	Attack type	Definition
Network layer	Spoofed, altered	Making routing loops, attracting or repelling network traffic from other nodes, changing routes, creating false error messages, and increasing delay
	Selective forwarding	Malicious nodes are created which forward and drop messages randomly
	Sinkhole	The nodes attract other nodes by sending high quality path information
	Sybil	The node is shown with more than one identity in the network
	Wormholes	A low-latency link between two portions of the network over which an attacker replays network messages
	Hello flood attacks	The attacker uses the low-latency link between two nodes to replay network messages

of harvesting energy from the environment. In addition, these surveillance systems will send real-time video streams over a set of heterogeneous networks to reach a central location for processing and analyzing the video streams. The context-aware ability of WSNs can also be integrated into the surveillance system, which will in turn enhance surveillance accuracy. Further, enhanced surveillance accuracy will lead to improved analysis and assessment of threats. For example, a context-aware surveillance system will be able to report whether toxic gas has leaked from a given facility while sending an image to the central location.

The following are recommended features for next-generation WMSNs:

(i) Context awareness: routing protocols should be designed to report sensed information with real-time video and audio streams to improve event detection.

(ii) Interconnection with other networks: the next-generation WMSNs are expected to be seamlessly integrated and interconnected with other networks and platforms (e.g., Internet of Things and cloud computing).

(iii) Long-lived sensor motes: the motes should be energy efficient and able to extend the network lifetime from months to years [19].

(iv) Very high throughput: the next-generation WMSNs should be able to transfer hundreds of real-time high-definition video streams. Therefore, the link throughput is expected to increase up to 1 Gbps [19].

(v) Mobility support: the sensor mote should also be mobile to efficiently cover large areas.

WMSNs security is also a major concern. It is important to protect data against unauthorized access and modification to ensure the availability of services. Also, if the collected data is private and sensitive, privacy issues are also of concern. To encourage the use of WMSNs in our daily lives, security and privacy issues should be addressed. The different types of network layer attacks in WMSNs are shown in Table 2.

The existing security mechanisms for WMSNs still have many issues and challenges that need to be addressed [20]. Many studies show that the findings on providing security in wireless sensor networks are not applicable to WMSNs because they have special multimedia characteristics and

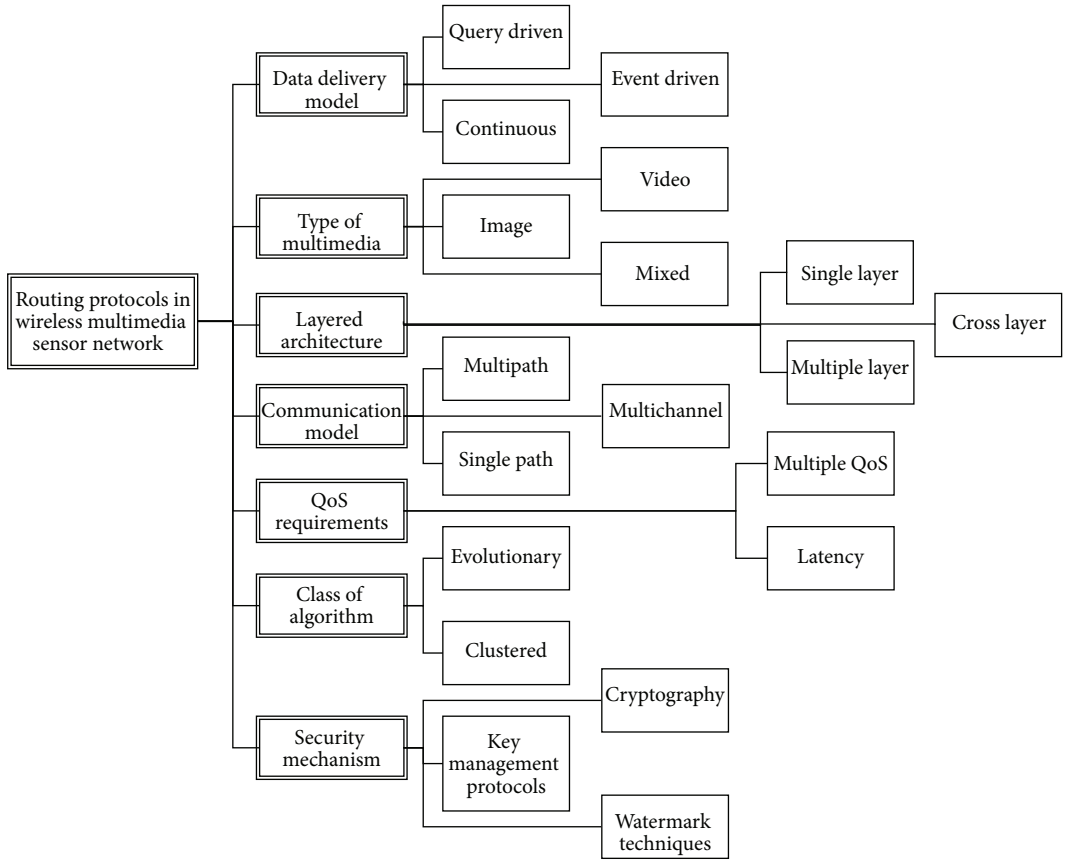

Figure 1: The classification of routing protocols for WMSNs.

requirements [21–23]. WMSNs also address privacy issues because multimedia sensors often carry private information about people or sensitive information about critical infrastructure. In the literature, there have been many surveys about security issues in WMSNs. Here, we discuss threats, attack types, threat resources, and security requirements. After that, we survey different security works proposed for WMSNs.

Designing secure routing protocols for WMSNs requires additional research in spite of the many routing protocols proposed for WSNs. According to the direction of the current research, we can classify the routing and security protocols into different categories as shown in Figure 1 [24]. There are many surveys reported in the literature [2, 18, 20, 24–27], but almost all of them focus on routing and related issues or security. No research has addressed the relationship between security and routing mechanisms in WMSNs. Ehsan and Hamdaoui [24] survey energy-efficient routing protocols for WMSNs and discuss performance issues for these techniques. Costa and Guedes [28] survey the studies on cross-layer-based techniques proposed for WMSNs and the benefits of using cross-layer designs in resource-constrained WMSNs. Almalkawi et al. [29] present the status and current challenges of studies on multimedia communication in WSNs.

The geographical routing protocols proposed for WMSNs are surveyed in [30], and the swarm-based routing protocols are surveyed in [31, 32], where the general principles of swarm intelligence and its application in routing are discussed. In [33], the challenges and opportunities of visual sensor networks (VSNs) are highlighted along with the main research issues such as camera coverage optimization, network architecture, and low-power visual data processing. However, many surveys on security issues and challenges are available in the literature. Grieco et al. [20] survey the primary security solution for WMSNs and the security mechanisms. These security mechanisms include authentication mechanisms, secure localization algorithms, and trust management.

Also, the researchers raised the topic of privacy issues, as well as secure techniques for the compression and aggregation of multimedia contents. In [34], the current security mechanisms for WSNs and the various types of attacks are discussed along with their countermeasures. Winkler and Rinner [18] present a comprehensive and extensive survey that includes the characteristics of VSN applications, as well as potential security threats and attacks and any major security challenges. The authors propose a new classification of data-centric, node-centric, network-centric, and user-centric security for VSNs. The security requirements for each aspect are presented with related work for each class. Also, privacy protection techniques and recent trends in VSN security and privacy are included.

The survey in [35] presents a study about current routing protocols for WSNs, given their security issues and design challenges. The authors explained different attack types of

routing protocols and provide a proposed solution to avoid such attacks. In [36], an analysis of the different security issues that affect the design of WMSNs platforms and protocols is provided. Also, the survey includes a discussion about the differences in security issues between WSNs and WMSNs. The future of security mechanisms in WMSNs is discussed, and the authors argue that the DoS attacks will continue to be one of the main security challenges in WMSNs. Furthermore, there are many specialized surveys about specific security issues. For example, in [37], physical attacks and trusted platforms in WSNs are discussed. In [38, 39], the recent intrusion detection systems are surveyed, while in [40] different types of selective forwarding attacks and their respective solutions are discussed. Finally, in [41], swarm intelligence in intrusion detection is surveyed.

Our review focuses on the proposed routing techniques. We also list the proposed security solutions for WMSNs to give an integrated perspective on current routing and security. We classify various routing techniques and security mechanisms according to the current research directions. Also, we present a comparison to discuss all the aspects of proposed works, identify current challenges, and highlight promising future research directions. The main contribution of this review is to examine the relationship between routing and security mechanisms in WMSNs.

The rest of the paper is organized as follows. In Section 2, we present an overview of design challenges and resource constraints for WMSNs. We classify and discuss the current security solutions for WMSNs in Section 3. In Section 4, we list current issues and future directions. Finally, we conclude the paper in Section 5.

2. Design Challenges and Resource Constraints

WMSNs requirements lead to numerous challenges when designing secure routing protocols amid resource constraints of traditional WSNs. This section discusses the main challenges that should be considered for efficient communication in WMSNs.

2.1. Energy Consumption. Multimedia applications produce high volumes of traffic, which require high transmission rates and processing capabilities. This leads to the consumption of more energy than that in traditional WSNs. For this reason, centralized power control policies, that is, energy harvesting equipped with photovoltaic cells, are mostly used in present multimedia applications instead of DC batteries. While energy consumption is one of the most important performance metrics in WMSNs, routing protocols designed for WMSNs should be aware of energy consumption to prolong the network lifetime [1].

2.2. QoS Requirements. QoS requirements differ according to different types of multimedia applications. QoS metrics like delay, bandwidth, reliability, and jitter must be taken into account. For example, many multimedia applications are time critical [42], because the multimedia traffic cannot normally tolerate delay.

2.3. Multimedia Coding Techniques. Transmission of multimedia content has long been associated with multimedia source coding techniques because of the large amounts of traffic generated by multimedia sources, such as cameras. The use of compression techniques certainly decreases the amount of information required to be transmitted. This, however, comes at the cost of the degradation of multimedia quality (i.e., distortion).

2.4. High Bandwidth Demand. Multimedia traffic demands high bandwidth. This high bandwidth requires new transmission techniques to provide the required bandwidth with an acceptable energy consumption level to optimize the resource-constrained nature of WMSNs. The use of multipaths or channels can be a solution to this issue.

2.5. Security Requirements. Images and videos collected by multimedia sensors are very sensitive. Thus, security and privacy are more important for WMSNs than they are for scalar sensors and data networks. WMSNs are more vulnerable to security risks because they use a broadcast medium with an error-prone communication channel. In addition, they are usually deployed in open areas without any central control. Thus, it is easy for attackers to monitor and jam the communication channel.

There are three primary types of attacks:

(i) Active attacks, in which an attacker aims to get full or partial control over WMSNs: in some cases, injecting control messages into the network allows the attacker to obtain some privileges.

(ii) Passive attacks, in which an attacker aims to illegally obtain and use data from the network: this type of attack usually is done by overhearing the communication channel.

(iii) Denial of services, in which an attacker aims to disrupt the services and the availability of WMSNs, which affects the network and the information provided to users: this is done by jamming the communication channel.

Threat Sources. The threats on a specific network can occur from the inside or the outside. The protection methods differ according to the sources of a threat. Encryption, authentication, or digital signatures can be used for outside threats. For inside threats, however, the attacker may have legal access to data and management facilities. In principle, insiders can perform the same attacks as outsiders. Therefore, the same security requirements apply.

Attack Manipulation. An attacker may target the hardware or software of WMSNs. Software attacks include change of installed software, while sometimes the attack reaches different layer protocols. Hardware manipulation will cause more damage to the network because it affects the electrical circuits of nodes like integrated circuits [18].

The security risks increase when a sensor network is integrated with the Internet. The aforementioned resource

constraints with multimedia sensors make the conventional security solutions based on heavy computing infeasible. This calls for existing solutions to be adapted to WMSNs requirements. The multimedia data (images or videos) obtained by multimedia sensors may include people's personal information, which is a violation of their privacy. Therefore, such information should be protected and used with defined rules. As a result, the proposed studies and protocols for security in WMSNs should address security, privacy, and QoS requirements [42]. The following are the main design challenges for security in WMSNs.

(i) Open Network Architecture. There are many applications where WMSNs are integrated with other networks (e.g., Wi-Fi or the Internet). This integration makes WMSNs more vulnerable to attacks [36].

(ii) Resource Constraints. All security techniques require more processing capabilities and memory consumption. Therefore, the techniques applied must balance between constraints and performance.

(iii) Limited Physical Control. There are many applications where the multimedia sensors are deployed in different environments. It may be difficult to physically reach the nodes after deployment. An attacker can physically reach these nodes and take the information stored in the sensors. Thus, the information stored in the memory should be encrypted.

(iv) Privacy. Multimedia data requires privacy, so personal information should not be misused when transmitting important information.

3. Routing Protocols for WMSNs

Because the network layer provides energy-efficient paths that meet QoS requirements, it is important to ensure QoS support for multimedia applications. In this section, we survey recent routing protocols proposed for WMSNs and critically discuss their features and limitations. Then, we present a general comparison. Routing protocols in WMSNs can be categorized based on their function and model. Some routing protocols adhere to the data delivery model because they are query driven, continuous, and event driven. Some of those protocols are built to handle various types of multimedia (e.g., images and videos) and are built for mixed traffic. The decision to route the data is generated by routing protocols that depend on parameters from a single layer (this can be a cross layer) and also from multiple layers (e.g., in layered architecture). The type of routing protocol depends on the communication model. For instance, it matters whether the data are forwarded on multiple paths or on a single path. In addition, it is important to note whether the data travel on multiple channels, as each channel switches signals. QoS requirements-based routing is performed to maintain the quality of the data. Some are classified based on the algorithm utilized (e.g., evolutionary, clustered). Security mechanisms or secure routing protocols transfer the data packets from the source to the destination using cryptography, key management protocols, and watermark techniques. In the discussion, the surveyed protocols are categorized in the manner shown in Figure 1.

3.1. Swarm Intelligence Routing Protocols. ACO algorithms are a class of metaheuristic algorithms that mimic the cooperative behavior of ants in a food search process to achieve complex computations. They have been proven to be very efficient in solving many different discrete optimization problems [43, 44]. Examples of such problems include the traveling salesman problem (TSP), the vehicle routing problem (VRP), and routing algorithms in mobile ad hoc networks. Rosati et al. [45, 46] mention that a distributed heuristic solution (i.e., ant routing) displays several features that render it particularly suitable for use in wireless sensor networks. These features are as follows: they are fully distributed and very simple; they are self-organizing and fault tolerant; and they adapt to all kinds of long-term variations in topology and traffic demand. In the following, we survey ACO-based routing protocols.

ASAR [47] is a QoS routing protocol for WMSNs based on the traditional ant algorithm. The ASAR selects optimal paths to meet QoS requirements for different types of services. These services are the following:

(i) R: event-driven service mode (delay and error intolerant). This requires low bandwidth and a high signal-to-noise ratio path.

(ii) D: query-driven service mode (delay tolerant but error intolerant). A congestion and high signal-to-noise ratio path may be used for this service.

(iii) S: stream query service mode (error tolerant but delay intolerant). A low-traffic and low signal-to-noise ratio path will be acceptable for this service.

The ASAR protocol features a cluster-based architecture and only addresses the routing scheme between the cluster heads and the sink node. Each cluster head generates ants for each type of service (R/D/S) to find different service-aware paths from a given source to a destination. These paths must meet QoS requirements and must be suitable for the traffic type. A probabilistic rule depending on the pheromone value of the paths is defined to determine the move from the current node to the next. The pheromone value is calculated based on delay, rate of packet loss, bandwidth, and energy consumption. The simulation results show that the efficiency of the proposed protocol depends on the service type. For instance, some types perform well in some QoS metrics, while other types suffer with regard to delay and energy consumption. There are also some drawbacks, such as the bottleneck problem of the hierarchical model and the optimal path setup due to congestion, which require extra considerations that affect network performance.

Rahman et al. [48] propose M-IAR, a biologically inspired routing protocol. M-IAR is a swarm intelligence-based algorithm exploiting the concept of ant colony optimization to optimize QoS metrics like delay, jitter, energy consumption, and packet survival rate. The protocol does not need to maintain the global state of the sensor nodes. The routing

decision is only based on neighborhood information. The effects of both the distance from the current node to the next hop and the remaining distance from the next hop to the sink are considered in the routing decision. First, the source node sends a forward ant, which uses a probability equation to find the probabilities of each of its neighbors. The packet is then forwarded to the neighbor with the highest probability. The same steps are repeated until the destination is reached. The forward ant will be killed if it visits more than one half of the nodes, which means that the path has a loop or is nonconvergent. When the forward ant reaches the destination successfully, the backward ant is created to reinforce the visited nodes by increasing the probability value. The proposed protocol can be configured for both acknowledgment-based and non-acknowledgment-based modes. The backward ant will acknowledge the path chosen by the forward ant. The simulation results for the M-IAR protocol were not compared with those of other related protocols. However, the protocol shows good performance in both jitter and delay, and it is able to find the shortest path. This leads to the decreased consumption of energy. The load balancing between nodes, which causes the holes problem when the energy of some nodes is depleted earlier than others, is not considered relevant. The protocol requires accurate geographic information of the nodes, which in turn increases the cost of deployment.

ALCOLBR [49] is a routing protocol based on ant colony optimization for load balancing and addressing the QoS requirements for WMSNs. The intracluster routing, on the one hand, is designed as a minimum spanning tree. The intercluster routing, on the other hand, is designed based on the ant colony optimization (ACO) algorithm, which seeks to find optimal and suboptimal paths to destination. The construction of a hierarchical routing tree to a cluster head with cluster members is done by using the minimum spanning tree (MST) algorithm. Intercluster routing is used to find all optimal and suboptimal paths using the ACO algorithm. Suboptimal paths are only employed when the amount of data exceeds the path flow threshold. In this case, both forward and backward ants are used. The forward ants are programmed to die when they reach the expiry time. In the process of moving from one node to the next, the forward nodes update the pheromone value using a local pheromone update rule. The highest-probability node will be chosen next. The same process is repeated until the second and the third suboptimal paths are found. To reinforce the optimal paths, the backward ant releases more pheromones in these paths based on a global pheromone rule. Then the transmission will start from the source to the destination. In the case of a node failure, the neighbor node will set the pheromone value to zero and send an error message to the source node. Afterwards, the source node will stop the transmission in this path and enable an alternate path for transmission. The simulation results show that the performance of the protocol is better with protocols such as AGRA [50], ACO-based multipath routing protocol [51], and M-IAR [48] in terms of delay and the node's lifetime. It also has better scalability and reliability. The drawbacks of the proposed work are the hierarchical model, which introduces a bottleneck problem, and the optimal path selection that requires additional calculation, which may decrease network performance.

Huang et al. [52] propose an ant colony routing algorithm called IP-ACRA. This algorithm aims to improve the classical ant algorithm, which is optimized by the initial pheromone distribution to improve convergence velocity and optimal path discovery. To enhance the scalability and make the algorithm suitable for large-scale sensor networks while prolonging the network lifetime, the proposed IP-ACRA is modified to IC-ACRA, which is a cluster-based algorithm. The performance metrics considered were delay, packet loss rate, bandwidth, and energy cost. The objective functions of the feasible path are designed to integrate and normalize all of the aforementioned performance metrics. The algorithm aims to find the optimum path to maximize the objective function. As mentioned above, improving the convergence velocity is one of the goals of the proposed algorithm. This is achieved by optimizing the initial pheromone value. We can establish node adjacency by constantly flooding the neighbor nodes with hello packets. The sink node broadcasts "hello" at the beginning. When the intermediate nodes receive the hello packets, they forward them and record the precedent node number in their adjacent table. The protocol assumes that the single path with better routing performance metrics has an earlier hello packet. The initial pheromone value set on each link is based on the priority of the recorded time stamp. The earlier adjacent node will have a higher priority, and a larger initial pheromone value will be set to the link. Every forward ant has a table wherein the visited nodes are saved in order to prevent looping. The probability equation of selecting the next node is based on the pheromone value and the heuristic function that depends largely on the remaining energy. Local and global pheromone values are updated. The global pheromone value is more important than the local one, because it uses the objective function as an indication of the value.

Because IP-ACRA's influence on network performance is not significant, the authors modified it to IC-ACRA, which downsizes the network scale and divides the sensor nodes into clusters. Each cluster has only one cluster head and at least one multimedia sensor. The cluster head can communicate with the sink node, while the other nodes communicate with each other within the cluster. IC-ACRA finds the local optimal path in each cluster. The simulation results show that the number of ants that obtain the final solution in IP-ACRA is larger than that of the classic ant routing algorithm. The convergence velocity of the proposed protocol is better than the classic ant algorithm, especially when the number of nodes exceeds 40. The performance results of routing metrics show that IC-ACRA outperforms IP-ACRA and Dijkstra's algorithm in every aspect. The performance evaluation of real video transmission shows that the delay in IC-ACRA is shorter than IP-ACRA. Additionally, it has better performance in real video data transmission than IP-ACRA.

Al-Zurba et al. [53] propose a routing algorithm to find the optimum path that has the minimum cost. The cost function calculations consider link energy consumption, link

quality, and link reliability. The energy consumption cost is calculated as the summation of communication energies, which is the transmission energy and the receiver node energy. Link reliability in the cost function is defined as the percentage of time that a link works properly, while the link quality is defined as the bit error rate on the link. The transition probability for forward ants to move from one node to the next depends on the pheromone value deposited on the link and the heuristic value given to the link, which is calculated based on the cost of the link. At the beginning, the initial pheromone value is set to be equal for all links, while the heuristic value of a link is the inverse of the link cost. The pheromone value is updated only on the links found by all the ants. The updated pheromone value is commensurate with the cost function of the links. The authors studied many parameters that have an impact on ACO performance. These include the number of ants, the weights for the cost function and transition probability, and the pheromone evaporation rate, as well as their impact on the time to find the optimum path. The results show that doubling the number of ants results in doubling the computation time needed to find the optimum solution. The probability of finding the optimum solution from the first iteration also increased. To find the optimum path, the heuristic value should be considered more important than the pheromone value. The simulation results show that, by increasing the transmission rate, the queuing delay is reduced. As a consequence, the loss percentage is decreased. Furthermore, the authors study the effect of the video encoding rate, which shows that the average queuing delay increases with the increase of the video frame encoding rate. Also, the large-loss percentage increases when the frame encoding rate increases. Increasing the event generation rate leads to an increase in the average queuing delay. The average queuing delay is a major reason that many packets are delayed beyond the established deadline. Even further, this delay also increases the percentage of losses.

Cai et al. [54] modify the ACO approach to solve the delay-constrained, maximum-energy residual ratio (DCEERR) QoS routing problem of WSNs. The proposed protocol named ACO-QoSR [54] aims to find the best path that meets the QoS requirement of WSNs and the appropriate balance between QoS requirements and complexity. The QoS metrics considered in the work are the transmission delay and energy conservation ratio, including an energy balancing factor. The routing process is achieved through three phases: the forward ant phase, the backward ant phase, and the maintenance phase. The forward ant starts at the source node by generating a number of forward ants, and these ants record their path information on their way to the destination. When a node receives a forward ant for the first time, it creates a record in its routing table and randomly selects one neighbor node as the next hop. If there is a record in the routing table, the next hop is selected according to the probability value, which depends on the pheromone and heuristic values of the link. The heuristic value on the link is defined as the ratio between the residual energy of the current node and the summary residual energy of all of the neighbor nodes. The source node adds the ant ID, which uniquely identifies a forward ant; this allows the nodes to distinguish duplicate packets. When the forward ant reaches its destination, it will be killed, and the backward ant will be generated. The backward ant carries the source node address, path information, and pheromone update value. The backward ant will use the energy residual ratio and the hop count that the forward ant collects. Using this ratio and count, the backward ant will be able to calculate the increment of the pheromone value. The pheromone update or increment will be in the paths that meet delay and energy requirements. In the route maintenance phase, every entry in the routing table has an expiration date. When the expiration date is reached, a new discovery phase will restart. A periodic hello message is used to maintain updated information about the connectivity of the neighbor nodes. If a link goes down during data transmission, the node will deactivate this link by setting the pheromone value to zero. Then, it will find other nodes in the neighbor table. To avoid constructing a dominant path, the proposed work limits the maximum and minimum pheromone values. When the approach is simulated, the results show that the average delays of the proposed protocol are less than those of the AODV and DSDV protocols. The routing overhead is also smaller. As a result, the path's normalizing energy is improved.

Cobo et al. [55] propose a hierarchical structure routing protocol based on ACO to satisfy QoS requirements and support power-efficient, multipath video packet scheduling. At the beginning, the sensor nodes are clustered into colonies. Afterward, the paths between clusters are found. Finally, the network traffic is transmitted through the routes discovered by the forward ants. The QoS metrics applied when selecting the optimum node are packet loss rate, available memory, queue delay, and remaining energy. The network consists of multimedia sensors (resource-rich nodes) and scalar sensors. The transmission power is dynamically adjusted, according to the distance between two nodes. A clustering algorithm is utilized to provide scalability, enhance network performance, and maximize network lifetime. The clustering process is based on a T-ant algorithm. This process is split into multiple rounds. Each round is composed of a cluster setup phase and a steady-up phase. In the cluster setup phase, the cluster heads are selected, and the clusters are placed around them. The data transmission between the sensors and the sink takes place during the steady phase. A special ant called the cluster ant is used to control the selection of the cluster heads. Only the node that has a cluster ant becomes a cluster head. The others join the best cluster head in their range. The ability to become a cluster head is determined by clustering the pheromone value of the node. This value is calculated based on the availability of both memory and energy. The sink node redeems a specific number of ants with a time-to-live (TTL) value. The TTL value is equal to the number of ants. The ants randomly choose one of their neighbors based on the probability function defined by clustering pheromone values. The pheromone value of the selected cluster head is decreased to avert the cluster head for the second time. If the cluster head recognizes a node that is three or more hops away, the neighbor of that node in the same path is selected to become a cluster head. Therefore, a better distribution of cluster heads in the network is guaranteed.

A packet scheduling policy is proposed to assign different priorities to different traffic classes. Three phases are proposed to achieve route discovery and data transmission. First, the forward ant phase starts by broadcasting forward ants. When the forward ants reach the next cluster head, the information fields are updated. Next, the same steps are repeated by forwarding the ant to the next cluster head on its way to the sink node, according to the probability value. The probability value (i.e., the pheromone value) is calculated as the summation of the QoS metrics (energy, delay, bandwidth, packet loss rate, and memory) that the forward ants collect. The backward ant is launched back in case the forward ants find paths that fulfill the application requirements. The routing maintenance phase deals with congestion and lost link problems. The behavior of the data ant is similar to that of the forward ant. Data ants are assigned to transport urgent or real-time data. This data is then processed before all of the other traffic classes in every node. AntSensNet offers a mechanism to transport a video stream between the source node and the sink node. This mechanism is based on the approach of Politis et al. [56] and uses an efficient, multipath video packet scheduling method. This method leads to minimal video distortion because it uses a video ant. The behavior in each intermediate node is the same as when discovering a single path, except that the intermediate node does not discard the duplicate video ants in order to discover a multipath. The simulation results show that the proposed protocol achieves a lifetime more than twice the cluster head of the T-ANT. ASNS shows a comparable average packet delivery ratio with AODV, while AntSensNet outperforms those two protocols after a few seconds. ASN and ASNM packets' delays are lower than those of AODV. The overhead of the proposed protocol is more than that of AODV due to the number of ants used. Also, the simulation results show that the video quality is higher than those of other multimedia protocols like TPGF and ASAR.

3.2. Geographic Routing Protocols. TPGF [57] is a two-phase, geographic, greedy forwarding algorithm for WMSNs. The first phase is responsible for exploring the possible routing paths while the second phase is responsible for optimizing the discovered routing paths with the least number of hops. The protocol assumes that each node is aware of its location and the location of its one-hop neighbor node. Each node has three states: (1) active and available, (2) active but unavailable, and (3) dead. The links have two states: available and unavailable. The routing paths should be through active and available nodes and available links to avoid the holes. Then, the found routing paths are optimized with the least number of hops. For these two phases, geographic forwarding and path optimization are proposed. The geographic forwarding is responsible for finding routing paths with bypassing holes. It uses two methods: greedy forwarding and "step back and mark." Greedy forwarding chooses the next-hop node closest to the sink among all neighbor nodes. "Step back and mark" works as follows: if the node has no next node except its previous node, it will mark itself as a block node. Then, the previous node will try to find another available node. An acknowledgment will be sent back to the source when the routing path reaches the destination. The acknowledgment will be sent to the node that has the same path number and the largest node number. The results show that, on average, TPGF finds more paths with shorter lengths than those found by relevant protocols like GG and RNG. The drawback of TPGF is that it needs to build a complete map of the network topology, which limits its scalability.

TPGF Plus [58] is an extension of TPGF, which uses the neighbor information of two hops for geographic routing and duty cycle assignments. Next, the closest node to the destination (among all of its one-hop and two-hop neighbors) is selected.

MPMPS [59] is also an extension of TPGF. MPMPS illustrates that not every path that TPGF finds is suitable for video transmission. This is because a long path with a high delay may not satisfy the time requirements for video transmissions. Also the protocol distinguishes between image and audio streams in videos. The priority is given to one over the other based on the application requirements. This allows it to guarantee that it will use a limited amount of bandwidth and energy.

GEAM [60] is a geographic, energy-aware, multipath routing protocol designed to address the problem of interfering between the multiple paths that are found. The sensor network area is divided into many district zones where the data are transmitted through the divided zone without interfering multiple paths. First, all the zones have the same load. After that, the loads for each zone are specified according to the energy level of the nodes in the zone. The transmission phase is divided into several runs. Each run has a fixed period and three rounds. In each round, only nodes of specific zones with optimal resources will participate in the transmission. To address the hole problem, transmission paths with dead zones will include detours.

AGEM [61] is an online geographical routing protocol designed for load balancing and minimizing energy consumption. It relies on beacon exchanges for neighborhood state maintenance. The smart greedy forwarding scheme is used for selecting the next hop, and the walking back forwarding mode is implemented to avoid holes. The neighbor nodes are selected by using an adaptive compass mechanism. The forwarding decision is based on the energy level, the number of hops, the distance between nodes and their neighbors, and the history of the packet that belongs to the same stream. The set of selected nodes is reduced to only those nodes with the best angular offset toward the destination.

GEAMS [62] is a geographical, multipath routing protocol designed to prolong the network lifetime. The proposed protocol is an enhancement of the GPSR protocol [63] wherein the feature of load balancing is added. This helps to reduce the queue size and increase the lifetime of the network. The forwarding decision policy is made based on the remaining energy, the number of hops, the distance between a node and its neighbors, and the history of the forwarded packet belonging to the same stream. There are two modes used by the proposed protocol: the smart greedy forwarding and the walking back forwarding. The first mode is used when there is always a neighbor closer to the destination than the

current node. The second mode is used to deal with a blocking situation. An example of a blocking situation is when the forwarding node cannot find the next hop node toward the destination. Each sensor node stores some information about it on the neighboring node, which includes the distance, link rate, and remaining energy. The simulation results show that the GEAMS is more suitable for WMSNs than the GPSR protocol. It ensures uniform energy consumption, and it also meets QoS constraints.

3.3. Routing Protocols Addressing Different Requirements. Lan et al. [64] propose a routing protocol that uses metadata to construct multipath routing to meet QoS metrics. The proposed protocol uses the advanced Dijkstra algorithm and a cost function to make routing decisions. The advanced Dijkstra algorithm reduces the number of neighbor nodes by excluding the nodes with insufficient remaining energy. In addition, the Dijkstra algorithm uses more than one factor, such as delay, bandwidth, and remaining energy. The cost function is calculated based on delay and energy consumption for multipaths, and then the optimized path will be selected. End-to-end delay calculation depends on two things: the distance between nodes and the processing and queuing delays of the relay nodes. To reduce queue delay, a classified queue model is introduced at each node to classify real-time data and non-real-time data. Metadata is used to describe the packets. Ordinary packets are distinguished by a unique ID and time stamp. However, multimedia packets are also assigned unique IDs with a time and location coordinator to avoid repeating the same data and thereby consuming more energy. The proposed protocol was simulated, and the results showed that it performed better than the SAR protocol in delays and energy consumption. The protocol does not consider reliability or bandwidth. The metadata is, however, inappropriate for multimedia data because it increases the overhead and energy consumption.

Sun et al. [65] propose a routing protocol for WMSNs using multipath and load balancing. They aim to increase the reliability, save more energy, and control congestion. The proposed protocol is flat and event driven. No global topology is required, and a sensor node is only aware of its neighbor nodes, which reduces the overhead. Three full disjoint paths are built from a source node to a sink. These are the primary, alternate, and backup paths. The primary path is the least-delay path, and it is followed by the alternate and backup paths. By default, the backup path will be used if the primary or alternative paths fail. The transmission on these paths will occur at a stable rate and in a "round robin" fashion, albeit with a specific time control called time slice control. Each sensor node will use two paths for transmission. As the primary path has less time delay, it will receive more time than the alternate path. The congestion control mechanism is designed for the major node (joint node), which is a node used by the two paths as a relay node. This mechanism monitors the queue of the node if the receiver queue reaches its threshold. A congestion notification is sent back to the source. Next, it will stop transmitting in this path and switch to the other path. The simulation results show that the protocol enhances the lifetime and throughput of the data packet. However, under a higher transmission rate, the receiving rate and the network lifetime quickly decrease. For this algorithm, the redundancy is low, which affects reliability. The study did not discuss the important metrics of delay and bandwidth, which have a greater impact on multimedia transmission.

Xie and Gu [66] propose multipath routing protocol to support hole bypassing, load balancing, and congestion controlling. The proposed algorithm consists of two phases. The first phase determines a set of multiple paths, while the second selects a routing path from the found paths. When it explores a path, a node that belongs to FCS (the set of nodes nearer to the destination than the current node) with less of the decisive energy factor (DEF) is selected as the next forwarding node. The proposed protocol uses a search algorithm that consists of a wave-front expansion and path backtracking. In the wave front, all of the valid nodes from the source to the destination are labeled in a decreasing tag number until the destination is reached. During path backtracking, the algorithm starts from the destination to the source and selects the node whose tag number is greater than that of the current node. When the source node is successfully reached, the path is built. Selecting paths randomly and independently from different sources increases the congestion and energy consumption in some nodes. A path selection strategy is designed to overcome these problems. To manage energy consumption, a decisive energy ratio change request (DERCR) message is introduced, which is sent by a node to the source to update the energy consumption value on the path. A control message containing the node and path ID is introduced to avoid congestion. When the queue exceeds the threshold specified by the user, the node sends this message to all of the nodes in the routing tables. Afterward, adjustment strategies are applied. Examples of adjustment strategies include gradual increase strategies based on the path and flows. However, the protocol was not simulated to show the performance. Delay, bandwidth, and jitter, which are tight requirements of multimedia transmission in a wireless sensor network, were not considered in the design.

Hamid et al. [16] present a multichannel, multipath, QoS-aware routing protocol. In this process, a dynamic adjustment of the required bandwidth and proportional delay differentiation for real-time data occurs. As a result, the routing decision in the proposed protocol is made. To efficiently utilize the bandwidth using multiple frequencies, a scheduling approach based on mutual orthogonal Latin square (MOLS) is applied to assign transmission and reception activities. Next, a packet scheduling policy is introduced, where every node has a classifier to send data into different queues, according to their bandwidth and delay requirements. Initially, the sink node will specify the bandwidth value depending on the delay of the time-critical packets and send this value to all of the nodes. After this occurs, all of the nodes will dynamically calculate their bandwidth value considering the distance to the sink. The path length-based proportional delay differentiation (PPDD) will calculate the delay for each packet in the queue along the path. The PPDD schedulers assign packets to classes and identify average proportional

hop-queuing delays between them at each node in the path. The proposed work transfers the packet over fewer numbers of hops to the sink to reduce the delay. To maximize the bandwidth of non-real-time traffic, the sink will observe the delay. If the delay increases, it will increase the bandwidth for real-time traffic and vice versa. Routing from the source to the destination will be done through the paths and channels that meet the bandwidth and delay requirements. Packets that do not meet the QoS requirements are discarded. The best-effort traffic will be routed through alternative paths for balancing the distribution of the remaining traffic. The simulation result shows that the proposed protocol has a good performance in delay, throughput, and lifetime compared to the protocol proposed in [67]. However, reliability and energy are not prevalent in the literature. In addition, a greater number of delays occur from switching between different frequencies.

MCRA [15] is a multiconstrained routing protocol designed to provide an end-to-end delay and packet loss ratio guarantee. In addition, this protocol also balances the energy consumption in sensor nodes. The proposed protocol is query driven and operates in a query-flooding data mode. The interest message is sent from the source node to all of the neighbors. When a certain node that meets the QoS requirements receives the message, it will broadcast the interest to all of its neighbors. Otherwise, it will discard it. The same steps are repeated until the interest reaches the source node. When the source node receives multiple interests from different paths, it will choose the optimum path. The differentiation service in the MAC layer can be used to classify the real-time data and best-effort data into different priorities. To decrease the redundancy and retransmission caused by collision, the proposed work introduces a message suppression technique, which consists of restraining forwarding and deferring. Restraining forwarding reduces the number of interests by restraining some nodes from performing forwarding operations. Deferring forwarding, however, involves deferring the forwarding action so that the nodes will have enough time to collect and merge interests from different sources. The authors design a localization approach based on hop-count information attained from the routing process. They also suppose that the network nodes are distributed on a plane of a rectangle with "m" units in length and "n" units in width. The simulation results show that the packet loss ratio in MCRA is the best compared to DD and SPEED [15] protocols. It was also observed that the end-to-end delay is quite close to that achieved by SPEED, while it outperforms SPEED in energy consumption, particularly when the number of nodes is greater than 70. However, the proposed work did not consider the reliability and bandwidth. Furthermore, it is not still energy efficient because of the flood methodology used to find the sink node.

Poojary and Pai [68] propose a routing protocol designed to be power aware and reliable, as well as to exhibit low latency. The routing algorithm consists of the route setup phase and the data transmission phase. In the route setup phase, a discovery message is sent by the source node to all of the neighbors to explore different paths. When the neighbor nodes receive the message, they will forward it to the next hop if the number of paths built through this node is less than the threshold and the residual energy of the node is more than the required energy. However, if it does not fit this set of requirements, the node will send a negative acknowledgment message. The same procedures are repeated until the message reaches its destination. Then, if the destination node is ready to receive data, it will send an "ok" message to the source node. When the "ok" message is received by the source node, it will add an "ok" message to the sender node ID of the multipath set. This consists of the nodes that are used as the next-hop nodes in transmission. In the data transmission phase, subsets of paths are selected based on the residual energy. The data is split into "m" parts and sent in multiple paths. To achieve reliability, the proposed protocol uses Reed Solomon encoding to encode the transmitted data. The simulation results show that the energy consumption is less than that achieved by conventional protocols. The packet loss ratio is decreased when the number of transmission paths is increased. Unfortunately, the use of Reed Solomon encoding for reliability increases energy consumption. Furthermore, no considerations for end-to-end delay and bandwidth requirements were made. Finally, splitting data into different paths increases the overhead of data collection.

Li et al. [69] propose a multipath routing protocol based on directed diffusion. The protocol tries to find multiple disjointed paths with high throughput and low end-to-end delay. For this purpose, the protocol uses a path metric cost based on delay and expected transmission account (ETX). The path metric cost also modifies directed diffusion protocol by the following: (1) using the path cost as a metric, instead of pure delay, and (2) reinforcing multiple paths at the sink to obtain disjointed paths from the source. When the source receives an interest from the sink, exploratory data packets are flooded. Then, the relay nodes will read SNR from the packet when they receive exploratory data. ETX of the previous three upstream links is calculated from SNR and inserted into the packet header of the ETX field. The cost of each subpath is kept in a local table on the intermediate nodes in ascending order. After this, the one with the lowest cost is forwarded to the next hop. For delay, the protocol only considers the packets whose timestamps satisfy the delay constraint. It is evident that the proposed protocol works efficiently in front of EDGE and directed diffusion protocols in both throughput and delay aspects. However, flooding still occurs during the exploring phase, which increases energy consumption.

Kai and Min [70] propose a reliable routing protocol based on the energy prediction of WMSNs. The sensors predict the energy levels of other nodes via this mechanism. Depending on prediction, the protocol can balance the energy consumption of the nodes by a power allocation mechanism. The main goals of the proposed protocol are to increase the reliability and balance the energy consumption. The reliable transmission rate is increased by increasing the power transmission level, which leads to the consumption of more energy. In order to save energy, the authors use the power control algorithm presented in [71, 72]. This algorithm guarantees reliability by gradually increasing power levels. If the maximum power level still does not meet the reliable

transmission request, another route needs to be built. The energy prediction mechanism is achieved by designing a state conversation model for intracluster nodes under the assumption that there are seven working states for sensors. Afterward, a Markov chain stimulates the working state. To make sure that all sensory data reach the sink, the network is divided into many concentric coronas. A corona's width is equal to the communication distance when using the lowest transmission power level. At the beginning, the power level is set to 1 for all nodes. If a node fails to find the next hop or does not meet the reliability requirements, it will increase the power level gradually until the maximum power level is reached. If it still fails, it will stop the processing and try to find another route. To balance the network energy consumption, the transmit power level is adjusted dynamically according to the remaining energy. The simulation results show that the energy prediction mechanism increases the node lifetime and enhances the reliability. However, the results were not compared to those of relevant protocols. It should also be noted that the energy prediction calculations also incur power consumption. Again, there was no consideration for delay and bandwidth.

LEAR [71] is an energy-aware multimedia routing protocol, which modifies the AODV protocol and offers QoS by assigning routes according to the data type that are less congested and have maximum power. The protocol also offers a hole bypassing technique. The protocol assumes that the network consists of scalar sensors and multimedia sensors. The scalar data is treated as the best-effort data. However, special care must be taken for multimedia data. A bit is inserted into the request message to distinguish between scalar data and multimedia data. When an event occurs, a request message is broadcast to all the neighbors of the source node. The node receiving this message again sends it to its neighbors until it reaches the destination. The destination replies by sending a request reply message to the source. When the source receives this message, the transmission will start along this path. The path selection is based on route selection factors. The node with a high selection factor value will be chosen as a forwarding node. The selection factor calculation is based on the remaining energy and active routes used by the node. When the node reaches 25% of its total energy, it will be labeled as a swap node and will not participate in the routing. The scalar data is routed like it is in the AODV protocol. The simulation results show that the number of paths increases as the amount of multimedia data increases. The hop distance will increase, but with high throughput, the congestion will be reduced. The protocol still uses broadcasting in all forwarding steps, which increases energy consumption. Delay, bandwidth, and reliability are not considered in the proposed protocol.

The data dissemination phase is used as the first step in many different routing protocols designed for WMSNs. Mohajerzadeh et al. [72] propose a data dissemination protocol for WMSNs named MLAF. The protocol aims to reduce the redundancy, prioritize the data according to their importance, and give attention to delay and energy consumption. MLAF considers the network as a virtual grid where every node is aware of its geographical position (cell). There are two types of nodes defined in each cell: internal nodes, which have all of their neighbors inside the cell, and edge nodes, which have at least one neighbor in another cell. Each packet has a field that registers the ID of the received nodes. If any node receives the packet and finds its ID on the list, the packet is destroyed. The proposed protocol uses two mechanisms for routing: directional forwarding and delay-sensitive forwarding. In directional forwarding, there are two priorities. First, for low-priority data, each grid cell should receive data from the southern cell, and the packet coming from other directions will be destroyed. Second, for high-priority data, each grid cell receives data from all of its neighbors. In delay-sensitive forwarding, there are also two different priorities, but the forwarding method is different. For high-priority traffic, MLAF will decrease the number of hops by increasing the transmission power, while the low-priority traffic will follow the normal routes. The simulation results show that the performance of the proposed protocol is better when compared to the LAF protocol; however, broadcasting at each node increases energy consumption, redundancy, and congestion. The protocol requires a grid arrangement, which is unsuitable for many applications of sensor networks. Generated results were not compared to those of well-known protocols for WMSNs.

3.4. Secure Routing Protocols. In this section, we survey existing security proposals in WMSNs. While many studies have been conducted for providing security in WSNs, not many exist for WMSNs. Most of the proposals for providing security in WSNs cannot be applied directly to WMSNs, but in some situations, we can apply some of them without any major modification. Here, we survey only those proposals that have been specifically designed for WMSNs. The proposed security studies in the literature are classified according to different criteria and security issues. For example, they could be related to the attack type, the potential threats in each layer, or the mechanism used to mitigate the security risks. In [18], a new classification scheme is proposed for security requirements in WMSNs, which is divided into four areas, as Figure 2 illustrates. In this survey, the proposed works are categorized according to the security mechanism used as shown in Figure 3. The most suitable security technique proposed for WMSNs is the watermarking technique because it is lightweight and does not require much memory [4, 12, 73]. This technique is considered an attractive alternative for WMSNs. Watermarking is the process of embedding information, which allows hidden copyright notices or other verification messages in digital audio, video, or image signals and document objects. The requirements of different watermarking techniques may vary according to the application at hand. Furthermore, there is no standard technique that satisfies different application requirements. Here, we first discuss the proposals that are based on watermarking techniques. Next, we include works based on other security techniques as given in Figure 2.

Wang et al. [4] propose a watermark technique for sensed image data. Specifically, they use two adaptive thresholds as a watermark key. There are many types of watermark generators, such as the median filter [5], 8-bit chip signal [7],

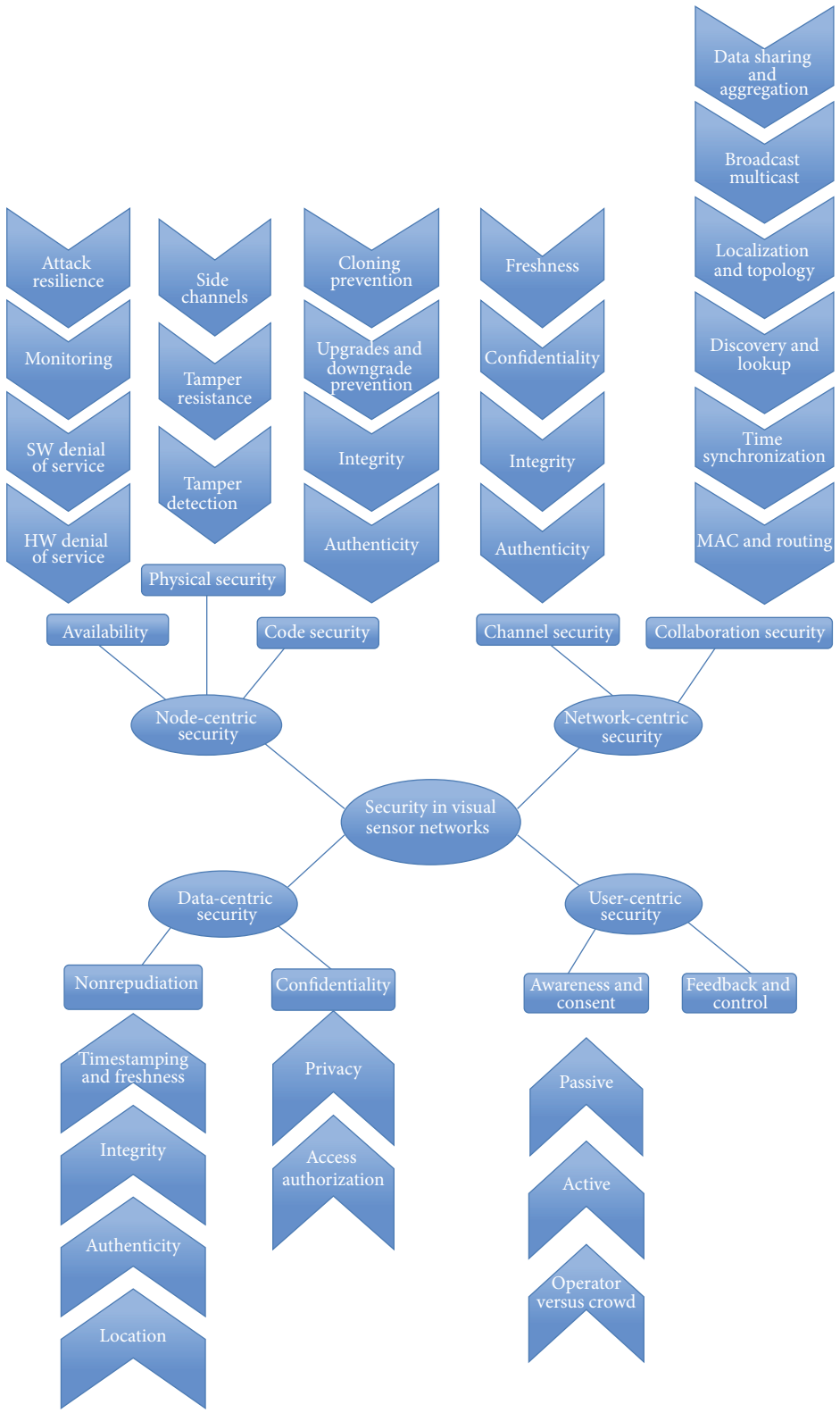

Figure 2: The classification scheme proposed in [18].

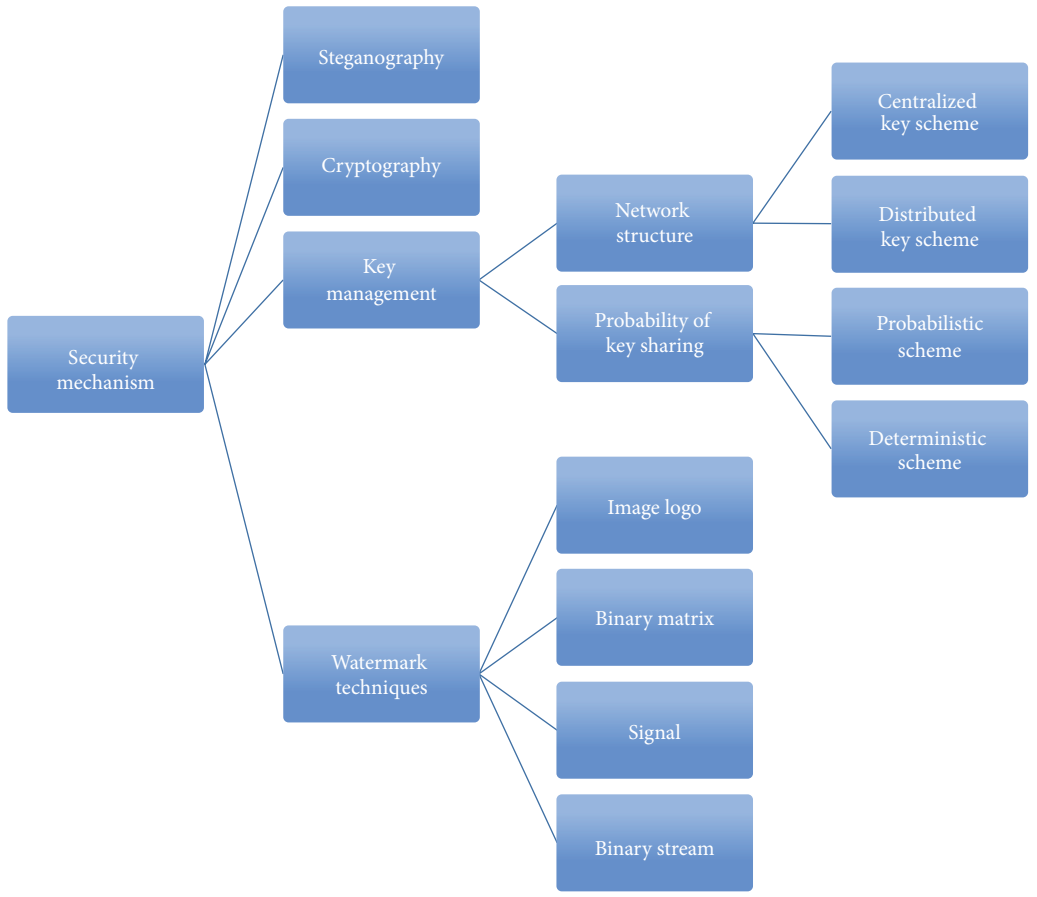

Figure 3: The general classification of security mechanisms.

and 5/8 encoder block [8]. However, the type of watermark generator used is not mentioned. The image logo is used as a watermark signal because it is more secure than a binary matrix.

Elbaşi and Özdemir [5] propose a security algorithm based on an energy-efficient watermarking technique that aims to secure data aggregation. A node puts the transmitted data into an image using an attack-resilient watermarking. The algorithm is cluster based and contains one sink node. The cluster heads aggregate data from all the nodes in their clusters. The secret data is embedded into images, which are obtained in the JPEG format, and the collected data is compressed via Huffman's coding. The authors assume that only numeric data are secret, while the images can be sent in the network without encryption. The aggregated images' data are compressed using discrete cosine transformation (DCT). The performance evaluation was done through simulation, and the method exhibited good results in terms of the similarity ratio and PSNR values.

Pingping et al. [6] propose a security watermark technique wherein images are used as sensed data, and the watermark is embedded into a low-frequency coefficient of discrete cosine transformation (DCT). The process begins by dividing the image into 8×8 blocks. Next, DCT is performed on each block. After that, the coefficient is selected at the location (Q, P) in each block of the blue component. Then, the chosen coefficient is replaced by the new watermark coefficient. Huffman's coding is performed, and the same steps are repeated for all the blocks. The extraction process is the reverse of the embedding process; in this event, the input is the watermark image in the JPEG format. To evaluate the work, the mean square error (MSR) and PSNR metrics were used. The experiments gave a result of PSNR = 45.5527, which indicates good quality. The watermark similarity was also recorded as 0.994, which means that the watermark scheme has good invisibility and can correctly extract the mark.

Wang [7] proposes a watermark scheme for multimedia authentication in a cross-layer manner. In this type of a scheme, the sensed data is an image, and the image logo is used as a watermark. Two adaptive thresholds are used as a watermark key, and the cover medium uses data packets and DWT as a transform domain. DWT is more robust because the watermark can be embedded into the selective coefficient at three levels of the discrete wavelet transformation. The adaptive threshold uses less power for WMSNs than others; in order to insert the watermark, its position is dynamically chosen according to the network condition. In this manner, energy efficiency and security are achieved. To evaluate the proposed scheme, drop packets are used as noise, and the vulnerable attack is an accidental type (e.g., compressing). Both the normalized correlation and PSNR were used to measure the similarity of the original watermark and the

extracted ones. The results showed that the scheme achieved very good invisibility. In addition, it is able to protect against JPEG loss compression.

Lin et al. [8] propose an energy-efficient distributed steganography scheme, which combines steganography techniques with the idea of distributed computing. The secretly sensed data is distributed among the sensor nodes. No node has a complete view of the original data. The massive computation can be shifted from sensor nodes to the sink node to prolong the sensor lifetime. The steganographic and steganalysis algorithm selects the middle-frequency coefficient in the DWT domain. After choosing the middle-frequency coefficient in the DWT domain, a perfect hash method is used to determine the specific position to embed the secret data. The proposed scheme uses LEACH as a routing protocol. Overall, although it is affected by noise and malicious attacks, the proposed method still achieves considerable robustness. Furthermore, it is more energy efficient than centralized steganography algorithms. The images will be more vulnerable to salt-and-pepper noise than the operation of cropping due to the middle-frequency coefficients.

The researchers in [14] propose a secure and selective encryption framework to optimize network lifetime and video distortion. The selective encryption of the video is done using H.264 standard video codec. Next the intraprediction mode is selected for encryption. Each picture is divided into 16×16 pixels' MB, and each MB is formed with luma and chroma components. An intramacroblock is coded without referring to any data outside the current slice, and there are Q prediction modes for a 4×4 luma block. The RC-5 is used for encryption. The simulation results show that the PSNR gain is significant compared with the traditional scheme. Furthermore, the increase of time due to encryption and decryption is acceptable. Finally, a timing analysis attack can be prevented.

Almalkawi et al. [9] propose a secure and cluster-based multipath routing protocol for WMSNs (SCMR). It takes advantage of the hierarchical structure with vigorous cluster heads. The multimedia QoS requirements are achieved by optimizing the multipath routing techniques. The cluster heads are responsible for finding and selecting an appropriate path for each type of data. The routing decision is based on the hop count and received signal strength. At the beginning, the sink node broadcasts a message that contains the ID of the sink node along with the related security information to authenticate communication with other nodes. The nodes join the cluster heads based on the signal strength. The node and link failure are detected by using acknowledgment messages. The lightweight distributed security mechanism is introduced based on the key management scheme to secure the communication channels between sensor nodes and protect the network against external attacks. Examples of external attacks include selective forwarding, acknowledgment spoofing, wormholes, and sinkhole attacks. On the other hand, internal attacks, such as spoofing or altering routing information, selective forwarding, and broadcasting hello floods, are disallowed. The cluster nodes are responsible for aggregating and encrypting data in each cluster. The proposed algorithm only supports authenticated encryption and authentication services. The decryption is done only at the sink node and at the cluster heads during the aggregation process. The algorithm implementation process starts by a preloaded master key when the sensor nodes are programmed with the intended software. Afterwards, each node computes its unique key shared between the nodes and the base station (BS). At the beginning, the BS authenticates it and subsequently authenticates other nodes using the master key. The protocol was simulated using NS-2. The results showed that using a different key type enhances protection from different attack types, such as selective forwarding, acknowledgment spoofing, wormholes, and sinkholes. Furthermore, the protocol is protected from inside attacks because it uses verified node identities by sharing an asymmetric unique node key.

Mulugeta et al. [10] propose a security scheme for the TPGF routing protocol, which aims to protect the routing protocol from vulnerabilities, such as greedy forwarding attacks, and prevent outside adversaries from joining the network. In addition, this scheme authenticates the control messages exchanged between nodes. In the initialization phase, the sink node generates and distributes private keys and public parameters. Afterwards, every node can calculate the public key of any node by knowing other nodes' IDs. Then, the secure neighbor discovery starts, aiming to prevent outside adversaries from joining the network. The proposed algorithm is not a perfectly designed version yet, as some difficult attacks still cannot be handled.

Lin et al. [11] propose ESR, a security routing scheme that aims to protect the network from internal attacks by assuming that the attacker can compromise sensor nodes and obtain their security information. The proposed protocol detects and bypasses the compromised nodes during the initial routing process. A trust evaluation model is introduced to protect the network from compromised sensor node's random attack behavior. The compromised nodes can tamper, drop, or flood the received packets to all neighbors.

Pingping et al. [6] propose a media-aware framework for facilitating various applications in the Internet of Things. The following are the fundamental goals of the media-aware framework: classifying and analyzing traffic for multimedia applications, developing media-aware traffic security architecture, and designing a scheme to evaluate the proposed work. The proposed architecture, which considers traffic analysis, security requirements, and traffic scheduling for multimedia applications, called MTSA, is designed to achieve good tradeoff between flexibility and efficiency. The multimedia traffic in IoT is divided into three categories: communication, computation, and services. MTSA has four major components. The first component is key management. In key management, a new classification uses two criteria: whether the multimedia traffic exercises control and whether the scheme is scalable or not. Accordingly, if computation and communication traffic at the sources increase dramatically with the size of the group, the scheme is treated as nonscalable. The second component is batch rekeying, during which there is a tradeoff between security improvement and computation complexity. The third component is authentication. In authentication, three levels of multimedia authentication

are used: group authentication, source authentication, and individual sender authentication. The fourth component is watermarking. During watermarking, it is recommended that a unique watermark is embedded for each user. This will prevent multiple users from receiving the same watermark in a network. Also, a distributed privacy paradigm of MTSA is provided. In this paradigm, the authority, cost, and encryption are obtained in a decentralized manner.

Suryadevara et al. [13] propose a secure framework for the transmission of a heterogeneous wireless sensor network related to the Internet of Things applications. This secure framework will provide solutions for challenging problems of multimedia applications in using secure heterogeneous communications. The proposed framework is called the multimedia data security algorithm for heterogeneous architecture (MDSAH). This design consists of two modules: the secured data transmission module and the traffic classification and analysis module. This framework aims to protect the data from unauthorized access. It primarily consists of two submodules: security and an authentication mechanism.

Next, a key generation technique is designed, which is randomly run to avoid duplication of keying. The design of the secret key generation is similar to the mechanism that is mentioned in [74]. The proposed mechanism considers group authentication and individual sender authentication. Traffic can be classified into two types: communication and computation. The communication rate depends on the distances of the nodes. Because the proposed mechanism is used in the home environment, all of the nodes are placed within the range of the coordinator. Reliability and flow control can be achieved by receiving the acknowledgement sent by the receiver to the sensor node. If the gateway buffer is not full, the acknowledgement is sent to the sensor node to engage in communication.

Traffic computation is the process of computing which packets are to be transmitted at which rate. This computation is based on the status of the gateway buffer capacity. MDSAH is simulated using the WiSE MNet simulator, which is based on Castalia/OMNeT++. The simulation uses smart home data as an input for MDSAH (scalar network data are utilized in the simulation). Further, a privacy system is proposed wherein the key exchange is decentralized. The performance focuses on delay and efficiency, each of which plays a significant role in the performance of an algorithm. The obtained results from the simulation show a good performance. Therefore, the proposed solution can be implemented for a wide range of aspects of real-time execution for the IoT using WSNs.

Porambage et al. [14] propose an implicit certificate-based authentication mechanism for WSNs in distributed IoT applications. The development of a two-phase authentication protocol allows the sensor nodes and the end user to authenticate each other. When they do so, they can initiate a secure connection. The design of the proposed solution is inspired by an ECQV implicit certificate scheme [14] and ECDH key exchange mechanism [75]. The main goal of the proposed work is to design and evaluate a two-phase authentication scheme for WSNs in distributed IoT applications. The protocol is lightweight, and it supports heterogeneity of the entities. End-to-end authentication in the application layer is proposed while relying on other security schemes in lower-layers communication. Subsequently, the edge devices and end users can mutually authenticate and establish a secure communication channel. Because of the distributed nature of the entire architecture, the proposed authentication mechanism contains two phases. The first phase is the registration phase. During this phase, the network obtains security credentials from a trusted party. The second phase is the authentication phase, which initiates trusted communication between two network entities using the obtained security credentials. The given solution is deployed in a network with Telsob sensors' nodes. The performance of the proposed scheme shows that it consumes less memory at each sensor node. This is due to the small size of its certificates. In addition, it offers better security. However, the proposed scheme still has limitations. For instance, node capture attacks can create a limited amount of harm to the entire network. Furthermore, the proposed work is secured only under node capture attacks.

Each sensor node computes the trust value of its neighbor's behavior and is responsible of local trust management. The process of detecting compromised nodes goes through three phases: (1) evaluating the behavior of neighbor nodes, (2) calculating direct trust value, and (3) calculating comprehensive trust value.

The behavior evaluation of a neighbor node starts when a sensor node sends data to a neighbor node. The Gaussian mixture model is used to evaluate the behavior of the neighbor nodes, and the whole operation is divided into a series of iterative processes by defining vectors to describe the historical and current behaviors of the neighbor nodes. The probability of the number of incorrect data forwarded from the first iterative process to the next iterative process is used to build the direct trust value. The direct trust value computes the trust value of the next neighbor, while a comprehensive trust value is used to compute trust value with indirect nodes. The routing metrics that are used to calculate the cost function of the next node are trust value, energy consumption, and history information of the neighbor node. The list of the recent state-of-the-art security solutions is given in Table 3.

Table 4 shows a summary of comparisons between the aforementioned routing protocols for WMSNs based on the QoS parameters considered: data delivery model, network architecture, hole bypassing, energy awareness, methodology used, congestion control mechanism, location awareness, and classification service.

Table 5 shows a simulated scenario of the proposed routing protocols for WMSNs. Based on the comparison study presented in the tables, we conclude that the routing protocols based on geographic and ACO algorithms perform better than other routing protocols following other algorithms. Also, the protocols that use delay and bandwidth as forwarding metrics are more suitable for multimedia transmissions.

In Table 6, the secure routing protocols have been compared to the next-generation features in WMSNs. This table shows that most of the protocols (Wang et al. [4],

Table 3: List of recent state-of-the-art security solutions.

	Tackled attacks at network layer	Security mechanism	Evaluation metrics
Wang et al. [4]	Cropping and compressing	Use two adaptive thresholds as a watermark key	Normalized correlation
Elbaşi and Özdemir [5]	Wormhole attacks, Sybil attacks, spoofing	Use watermarking technique to secure data aggregation	PSNR
Pingping et al. [6]	Salt-and-pepper noise and cropping	Watermark is used with the low frequency coefficients of DCT	PSNR
Wang [7]	Accidental type such as compressing	Two adaptive thresholds are used as a watermark key	Normalized correlation, PSNR
Lin et al. [8]	Malicious attack	Steganography technique with the concept of distributed computing	Normalized correlation, PSNR
Almalkawi et al. [9]	Selective forwarding, acknowledgment spoofing, wormhole, and sinkhole	Lightweight distributed security mechanism of key management	Scalability, SNR, BER
Mulugeta et al. [10]	Greedy forwarding, wormhole attacks, Sybil attacks	Security scheme for TPGF routing protocol using noninteractive key distribution scheme (ID-NIKDS)	Effect of malicious nodes on the routing paths
Lin et al. [11]	Can tamper, drop, or flood packets	Trust evaluation model based on Gaussian mixture model (GMM)	Detection accuracy ratio and false alarm ratio
Zhou and Chao [12]	Active inside attack, eavesdropping	Key management, batch rekeying, authentication, and watermarking	Complexity of multimedia computations and size of shares
MDSAH [13]	Attacks targeting authentication service	Key management with decentralized key exchange	Delay and efficiency
Porambage et al. [14]	Denial of service (DOS) attacks	Implicit certificate scheme and key exchange mechanism	Memory consumption

Elbaşi and Özdemir [5], Pingping et al. [6], Wang [7], Lin et al. [8], Varalakshmi et al. [17], and Lin et al. [11]) that have been proposed thus far are only for WMSNs. Only a few of the recently proposed protocols (Zhou and Chao [12], MDSAH [13], and Porambage et al. [14]) have been developed to maintain and secure the data traffic over a heterogeneous network. In addition, the architectural design in [73] considers long-lived nodes using energy harvesting and supports mobility. Still, none of these secure routing protocols have been experimentally tested.

4. Open Issues and Future Directions

WMSNs applications are in a constant state of dynamic evolution with much more opportunities for their deployment. It is important to note that, despite the huge number of studies in the field of routing protocols and security, there still exist many open issues that require urgent solutions. In the following, we discuss the open issues and outline future research directions for current and next-generation WMSNs.

(i) Multipath Routing. Reliability, security, and load balancing, which are critical in resource-constrained networks like WMSNs, can be improved using multipath routing techniques. Single-path routing, especially for multimedia transmission, degrades video quality. The best alternative for multimedia transmission is to divide and multiplex the encoded video data. Afterward, the sink node will assemble the parts to obtain the full information. Bandwidth utilization can be achieved using multipath routing techniques.

(ii) Multichannel Techniques. The availability of multiple frequency channels on modern radios has given users the opportunity to enhance the network performance. The hardware platform of many sensors can communicate on multiple channels, as mentioned in IEEE 802.15.4. It is very important to introduce channel switching to next-generation WMSNs architectures. In spite of the lack of an architectural consistency, using multiple channels will enhance network throughput and decrease the intranetwork performance. As a result, the external interface will be eliminated.

(iii) New Class of Algorithms. ACO and game theory-based routing protocols are gradually gaining the attention of researchers. These tools and algorithms are adaptive to the changes that appear in routing topologies, which helps with the adaptation of dynamic scenarios. The applicability of other algorithms based on supervised and reinforcement learning needs to be investigated for adoption in WMSNs routing protocols.

(iv) Cross-Layer Design in WMSNs. Recent empirical studies have indicated that the properties of low-power radio transceivers and wireless channel conditions must be considered in the design of protocols. The routing protocols based on reference-layered communication architecture are

Table 4: Summary of comparison between the aforementioned routing protocols for WMSN based on the QoS parameters considered: data delivery model, network architecture, hole bypassing, energy awareness, methodology used, congestion control mechanism, location awareness, and classification service.

Protocol	Architecture		Data delivery model			Location awareness	Hole bypassing	Methodology				Congestion control	Classification service	Energy efficiency	QoS parameters considered
	Flat	Hierarchical	Query driven	Event driven	Stream query			Multipath	Multichannel	Geographic	Other				
ASAR		√	√	√	√	√	√	√			ACO		√	√	Delay, packet loss ratio, bandwidth
Rahman et al.	√		√								ACO			√	Delay, jitter
ALCOLBR		√	√					√			ACO	√		√	Reliability
IC-ACRA		√	√					√			ACO			√	Delay, bandwidth, packet loss ratio
Hiba Alzubra	√		√								ACO			√	Link quality, reliability
ACO-QoSR	√			√			√	√			ACO			√	Delay and energy
AntSensNet		√	√	√			√	√			ACO	√	√	√	Delay, memory, bandwidth
TPGF	√		√			√	√	√		√					Delay, reliability
GAMES	√		√				√			√	Based on GPSR			√	Delay, reliability
Yao et al.	√		√					√			Metadata + advanced Dijkstra		√	√	Delay
Gunan et al.	√			√				√				√		√	Reliability
MandeXe	√		√				√	√			Amazing Algorithm	√	√	√	Reliability
Hamid et al.	√		√					√	√				√		Delay, bandwidth
MCRA [15]	√		√			√					Flooding		√	√	Reliability
Poojary	√		√					√						√	Reliability
Shuang et al.	√		√					√			Based on direct diffusion				Delay

Table 5: The simulation scenario of routing protocols for WMSNs.

Protocol	Verified method		Simulator type	Performance metrics	Compared to	Comparison result
	Simulator	Testbed				
ASAR	√		NS-2	Queuing delay, PRR, and dropped rate	Traditional ant-based directional diffusion routing algorithm (DD), Dijkstra	Select the optimal paths to meet their individual QoS requirements, thus improving network performance.
M-IAR	√		Java	Delay, jitter	Not compared	M-IAR shows good performance which achieves acceptable delay, jitter, and energy consumption.
ALCOLBR	—		NS-2	Delay, node lifetime, PRR	AGRA and M-IAR	ACOLBR has a better adaptability; it can achieve load balancing, reduce the end-to-end delay, and prolong the network lifetime.
IC-ACRA	√		NS-2	Delay, packet loss rate, energy, bandwidth	Dijkstra	It shows good result compared to Dijkstra in all the considered performance metrics.
Hiba Alzubra	√		Not specified	Link quality, link reliability, energy	—	The simulation studies the effect of changing number of ants, the importance of pheromone value, and evaporation rate. The effects of transmission bit rate and event generation rate are examined.
ACO-QoSR	√		NS-2	Energy	EEABR	It offers significant reductions of energy consumption and prolongs network lifetime.
AntSensNet	√		NS-2	Delay, packet loss, energy, memory	T-ANT, AODV, TPGF, ASAR	It outperforms AODV in delivery ratio, delay, and routing overhead. The video quality is better than ASAR and TPGF.
TPGF	√		NetTopo	Delay, number of found paths	GPSR	Holes can be efficiently bypassed compared to GPSR, suitable for multimedia transmission.
GAMES	√		OMNeT++	Delay, lost packet, energy distribution	GPSR	It is more suitable for WMSNs than GPSR as it ensures uniform energy consumption and meets the delay and packet loss constraint.
Yao et al.	√		Not specified	Energy consumption, delay, distance	SAR	The REAR algorithm prolongs the network lifetime and performs much better than SAR.
Gunan et al.	√		OMNet++	PRR, network lifetime	MHC and flooding	It achieves higher data rate and longer network lifetime. But under higher package transmit rate from source, receiving rate and network lifetime will drop fast.
Hamid et al. [16]	√		NS-2	Delay, node lifetime, throughput	Single-r and multi-r mechanisms	It provides significant performance improvements in terms of average delay, average lifetime, and network throughput.
MCRA [15]	√		NS-2	Delay, packet loss ratio, control message overhead	SPEED-DD	It shows that it has a good overall performance.
Poojary	—		Qualnet network simulator	Energy consumption, PRR	Not specified	It prolongs the network lifetime and the packet drop reduces as the number of paths selected for the data transmission is increased.
Shuang et al.	√		NS-2	Throughput, delay, goodput	EDGE and basic diffusion	It achieves high throughput and desirable delay to meet the QoS requirement of multimedia streaming.

Table 6: Comparison of secure routing protocols with respect to the next-generation features in WMSNs.

	Context-aware sensing	Interconnection with other networks	Long-lived sensor motes	Very high throughput	Mobility support
Wang et al. [4]	Sensed image data	No	No	No	No
Elbaşi and Özdemir [5]	Video or image data	No	No	No	No
Pingping et al. [6]	Image data	No	No	No	No
Wang [7]	Image	No	No	No	No
Lin et al. [8]	Image data	No	No	No	No
Varalakshmi et al. [17]	Multimedia semantic information and video content	No	No	No	No
Lin et al. [11]	General packets	No	No	No	No
Zhou and Chao [12]	Multimedia traffic of three categories: preference data, situation data, and capability data	Yes	Yes	No	Yes
MDSAH [13]	Networks with sensors capturing complex vectorial data, such as video and audio	Yes	No	No	No
Porambage et al. [14]	General data	Yes	No	No	No

not particularly efficient. This is primarily because the energy of the nodes along the video stream path is quickly depleted. It is extremely important to combine the characteristics of multimedia and information security at the application layer with gains and optimization at a lower layer in a cross-layer design. When consolidated with other layer functionalities, such a routing design can provide powerful solutions to many unresolved issues.

(v) Energy Efficiency. The major challenge for the reproduction of WMSNs is energy. In WMSNs, the importance of energy efficiency and QoS requirements should be balanced. The problem of finding optimal solutions that balance energy efficiency and QoS can be solved by using energy-harvesting mechanisms, which can significantly prolong the lifespan of the network or even allow it to perpetually run. The challenge of any sensor mote equipped with energy-harvesting capability is to keep its energy dissipation rate less than its harvesting rate. Thus, when the energy constraint is dropped, the optimization problem becomes less complex. This allows it to focus on optimizing other performance metrics, such as QoS.

(vi) Security Issues. In WMSNs, more data are carrying private and important information to the sink. This makes the issue of security essential. In this respect, secure routing is an issue that needs additional attention. It should, however, be noted that, with integrated security mechanisms, optimizing performance becomes another issue. The majority of the current studies focus on individual issues, while QoS requirements of WMSNs and security need to be jointly solved in an integrated architecture. This is because there is still a lack of approaches that consider privacy and security in a holistic way, and there are undefined rules to determine which security approach has improved performance. Furthermore, there is still no clear standard for the privacy principles, as the issue also impacts various personal and community cultures and attitudes.

(vii) Integration with the Internet and Other Wireless Technologies. The basis of business in wireless sensor networks is to make the information obtained by a sensor network available to people by means of an access medium, such as the Internet. The users of the Internet can inquire about different information. Thus, WMSNs will be remotely accessible via other networks and platforms, such as the Internet of Things, cloud, and radiofrequency identification (RFID). Hence, WMSNs need to be integrated with the Internet architecture. It is recommended to use the application level gateways or overlay IP networks as means of integration between WSNs and the Internet. Also, it is necessary to achieve integration with other wireless technologies without sacrificing the efficiency of each individual technology.

(viii) Context-Aware Sensing in WMSNs. Integrating sensing information into a real-time routing protocol can make the surveillance systems more intelligent and capable of distinguishing urgent matters that require human intervention from irrelevant events to the application at hand. In this case, the challenge is how to design an efficient threat assessment

system based on the video and audio streams, as well as the data collected from the environment.

(ix) Mobility Support. The mobility of sensor nodes can help to ensure full coverage and surveillance of the target area with a smaller number of nodes. The challenge in this case is how to select the node trajectory so that the important events are not missed.

5. Conclusion

The advent of WMSNs enables new applications to be created, and many research issues have emerged which require different and innovative solutions. In this paper, WMSNs technologies have been introduced, and the related challenges for current and next-generation networks are discussed. We have then classified current routing protocols according to the existing directions of the research. Furthermore, the performance issues of each routing protocol have been highlighted and compared. In addition, we have discussed the security issues and challenges. In line with this, the most recent works in security solutions for WMSNs are surveyed. With the increased need for more multimedia data content, the issue of secure multimedia routing in WMSNs is an area that needs urgent attention.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The authors extend their appreciation to the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia, for funding this work through the international research group Project no. IRG14-07B.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[2] I. F. Akyildiz, T. Melodia, and K. R. Chowdury, "Wireless multimedia sensor networks: a survey," *IEEE Wireless Communications*, vol. 14, no. 6, pp. 32–39, 2007.

[3] W. Yong, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, pp. 2–23, 2006.

[4] H. Wang, D. Peng, W. Wang, H. Sharif, and H.-H. Chen, "Energy-aware adaptive watermarking for real-time image delivery in wireless sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '08)*, pp. 1479–1483, May 2008.

[5] E. Elbaşi and S. Özdemir, "Secure data aggregation in wireless multimedia sensor networks via watermarking," in *Proceedings of the 6th International Conference on Application of Information and Communication Technologies (AICT '12)*, pp. 1–6, October 2012.

[6] Y. Pingping, Y. Suying, X. Jiangtao, Z. Yu, and C. Ye, "Copyright protection for digital image in wireless sensor network," in *Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '09)*, pp. 1–4, IEEE, Beijing, China, September 2009.

[7] H. Wang, "Communication-resource-aware adaptive watermarking for multimedia authentication in wireless multimedia sensor networks," *The Journal of Supercomputing*, vol. 64, no. 3, pp. 883–897, 2013.

[8] Q. Lin, R. Wang, N. Ye, and Z. Wang, "Energy efficient distributed steganography for secure communication in wireless multimedia sensor networks," *Journal of Electronics*, vol. 30, no. 1, pp. 9–16, 2013.

[9] I. T. Almalkawi, M. G. Zapata, and J. N. Al-Karaki, "A secure cluster-based multipath routing protocol for WMSNs," *Sensors*, vol. 11, no. 4, pp. 4401–4424, 2011.

[10] T. Mulugeta, L. Shu, M. Hauswirth, M. Chen, T. Hara, and S. Nishio, "Secured two phase geographic forwarding protocol in wireless multimedia sensor networks," in *Proceedings of the 53rd IEEE Global Communications Conference (GLOBECOM '10)*, pp. 1–6, December 2010.

[11] K. Lin, X. Ge, X. Wang, C. Zhu, and H.-G. Ryu, "Research on secure data collection in wireless multimedia sensor networks," *Computer Communications*, vol. 35, no. 15, pp. 1902–1909, 2012.

[12] L. Zhou and H.-C. Chao, "Multimedia traffic security architecture for the internet of things," *IEEE Network*, vol. 25, no. 3, pp. 35–40, 2011.

[13] J. Suryadevara, B. Sunil, and N. Kumar, "Secured multimedia authentication system for wireless sensor network data related to internet of things," in *Proceedings of the 7th International Conference on Sensing Technology (ICST '13)*, pp. 109–115, IEEE, Wellington, New Zealand, December 2013.

[14] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Yliant-tila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '14)*, pp. 2728–2733, IEEE, Istanbul, Turkey, April 2014.

[15] X. Yan, L. Li, and F. J. An, "Multi-constrained routing in wireless multimedia sensor networks," in *Proceedings of the International Conference on Wireless Communications & Signal Processing (WCSP '09)*, pp. 1–5, November 2009.

[16] M. A. Hamid, M. M. Alam, and C. S. Hong, "Design of a QoS-aware routing mechanism for wireless multimedia sensor networks," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '08)*, pp. 800–805, December 2008.

[17] L. M. Varalakshmi, G. F. Sudha, and G. Jaikishan, "A selective encryption and energy efficient clustering scheme for video streaming in wireless sensor networks," *Telecommunication Systems*, vol. 56, no. 3, pp. 357–365, 2013.

[18] T. Winkler and B. Rinner, "Security and privacy protection in visual sensor networks: a survey," *ACM Computing Surveys*, vol. 47, no. 1, article 2, 2014.

[19] H. Xu, L. Wang, and H. Xie, "Design and experiment analysis of a Hadoop-based video transcoding system for next-generation wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 151564, 7 pages, 2014.

[20] L. A. Grieco, G. Boggia, S. Sicari, and P. Colombo, "Secure wireless multimedia sensor networks: a survey," in *Proceedings of the 3rd International Conference on Mobile Ubiquitous Computing, Systems, Services, and Technologies (UBICOMM '09)*, pp. 194–201, October 2009.

[21] J. Sen, "A survey on wireless sensor network security," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 1, no. 2, pp. 59–82, 2009.

[22] N. Lasla, A. Derhab, A. Ouadjaout, M. Bagaa, and Y. Challal, "SMART: Secure Multi-pAths Routing for wireless sensor neTworks," in *Ad-Hoc, Mobile, and Wireless Networks*, vol. 8487 of *Lecture Notes in Computer Science*, pp. 332–345, Springer International Publishing, Cham, Switzerland, 2014.

[23] A. Derhab, A. Bouras, M. R. Senouci, and M. Imran, "Fortifying intrusion detection systems in dynamic Ad Hoc and wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 608162, 15 pages, 2014.

[24] S. Ehsan and B. Hamdaoui, "A survey on energy-efficient routing techniques with QoS assurances for wireless multimedia sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 265–278, 2012.

[25] M. Abazeed, N. Faisal, S. Zubair, and A. Ali, "Routing protocols for wireless multimedia sensor network: a survey," *Journal of Sensors*, vol. 2013, Article ID 469824, 11 pages, 2013.

[26] M. AlNuaimi, F. Sallabi, and K. Shuaib, "A survey of wireless multimedia sensor networks: challenges and solutions," in *Proceedings of the International Conference on Innovations in Information Technology (IIT '11)*, pp. 191–196, April 2011.

[27] A. K. Pathan, L. Hyung-Woo, and H. Choong Seon, "Security in wireless sensor networks: issues and challenges," in *Proceedings of the 8th International Conference Advanced Communication Technology (ICACT '06)*, pp. 1043–1048, February 2006.

[28] D. G. Costa and L. A. Guedes, "A survey on multimedia-based cross-layer optimization in visual sensor networks," *Sensors*, vol. 11, no. 5, pp. 5439–5468, 2011.

[29] I. T. Almalkawi, M. G. Zapata, J. N. Al-Karaki, and J. Morillo-Pozo, "Wireless multimedia sensor networks: current trends and future directions," *Sensors*, vol. 10, no. 7, pp. 6662–6717, 2010.

[30] Z. Li, R. Li, T. Pei, Z. Xiao, and X. Chen, "Survey of geographical routing in multimedia wireless sensor networks," *Information Technology Journal*, vol. 10, no. 1, pp. 11–15, 2011.

[31] M. Saleem, G. A. Di Caro, and M. Farooq, "Swarm intelligence based routing protocol for wireless sensor networks: survey and future directions," *Information Sciences*, vol. 181, no. 20, pp. 4597–4624, 2011.

[32] K. Saleem, N. Fisal, S. Hafizah, S. Kamilah, and R. Rashid, "Biological inspired self-optimized routing algorithm for wireless sensor networks," in *roceedings of the IEEE 9th Malaysia International Conference on Communications with a Special Workshop on Digital TV Contents (MICC '09)*, pp. 305–309, December 2009.

[33] Y. Charfi, N. Wakamiya, and M. Murata, "Challenging issues in visual sensor networks," *IEEE Wireless Communications*, vol. 16, no. 2, pp. 44–49, 2009.

[34] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 2, pp. 52–73, 2009.

[35] A. M. El-Semary and M. M. Abdel-Azim, "New trends in secure routing protocols for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 802526, 16 pages, 2013.

[36] M. Guerrero-Zapata, R. Zilan, J. M. Barceló-Ordinas, K. Bicakci, and B. Tavli, "The future of security in Wireless Multimedia Sensor Networks: a position paper," *Telecommunication Systems*, vol. 45, no. 1, pp. 77–91, 2010.

[37] Y. M. Yussoff, H. Hashim, R. Rosli, and M. D. Baba, "A review of physical attacks and trusted platforms in wireless sensor networks," *Procedia Engineering*, vol. 41, pp. 580–587, 2012.

[38] K. Saleem, N. Fisal, M. S. Abdullah, and S. H. S. Ariffin, "Biological inspired secure autonomous routing mechanism for wireless sensor networks," *International Journal of Intelligent Information and Database Systems*, vol. 5, no. 4, pp. 313–337, 2011.

[39] A. H. Farooqi and F. A. Khan, "Intrusion detection systems for wireless sensor networks: a survey," in *Communication and Networking*, pp. 234–241, Springer, 2009.

[40] L. K. Bysani and A. K. Turuk, "A survey on selective forwarding attack in wireless sensor networks," in *Proceedings of the International Conference on Devices and Communications (ICDeCom '11)*, pp. 1–5, February 2011.

[41] C. Kolias, G. Kambourakis, and M. Maragoudakis, "Swarm intelligence in intrusion detection: a survey," *Computers & Security*, vol. 30, no. 8, pp. 625–642, 2011.

[42] J. Zheng and A. Jamalipour, *Wireless Sensor Networks: A Networking Perspective*, John Wiley & Sons, 2009.

[43] K. Saleem, N. Fisal, and J. Al-Muhtadi, "Empirical studies of bio-inspired self-organized secure autonomous routing protocol," *IEEE Sensors Journal*, vol. 14, no. 7, pp. 2232–2239, 2014.

[44] K. Saleem and N. Fisal, "Energy efficient information assured routing based on hybrid optimization algorithm for WSNs," in *Proceedings of the 10th International Conference on Information Technology: New Generations (ITNG '13)*, pp. 518–524, April 2013.

[45] L. Rosati, M. Berioli, and G. Reali, "On ant routing algorithms in ad hoc networks with critical connectivity," *Ad Hoc Networks*, vol. 6, no. 6, pp. 827–859, 2008.

[46] K. Saleem and N. Fisal, "Enhanced Ant Colony algorithm for self-optimized data assured routing in wireless sensor networks," in *Proceedings of the 18th IEEE International Conference on Networks (ICON '12)*, pp. 422–427, IEEE, Singapore, December 2012.

[47] Y. Sun, H. Ma, L. Liu, and Y. Zheng, "ASAR: an ant-based service-aware routing algorithm for multimedia sensor networks," *Frontiers of Electrical and Electronic Engineering in China*, vol. 3, no. 1, pp. 25–33, 2008.

[48] M. A. Rahman, R. G. Aghaei, A. El Saddik, and W. Gueaieb, "M-IAR: biologically inspired routing protocol for wireless multimedia sensor networks," in *Proceedings of the IEEE International Instrumentation and Measurement Technology Conference (IMTC '08)*, pp. 1823–1827, May 2008.

[49] J. Bi, Z. Li, and R. Wang, "An ant colony optimization-based load balancing routing algorithm for wireless multimedia sensor networks," in *Proceedings of the IEEE 12th International Conference on Communication Technology (ICCT '10)*, pp. 584–587, November 2010.

[50] R. Xiu-Li, L. Hong-Wei, and W. Yu, "Multipath routing based on ant colony system in wireless sensor networks," in *Proceedings of the International Conference on Computer Science and Software Engineering (CSSE '08)*, pp. 202–205, IEEE, Wuhan, China, December 2008.

[51] K. Saleem, N. Fisal, S. Hafizah, S. Kamilah, and R. A. Rashid, "Ant based self-organized routing protocol for wireless sensor networks," *International Journal of Communication Networks and Information Security*, vol. 1, no. 2, pp. 42–46, 2009.

[52] H. Huang, X. Cao, R. Wang, and L. Sun, "A novel clustering ant-based QOS-aware routing algorithm in large scale

wireless multimedia sensor networks," in *Proceedings of the IEEE International Conference on Cluster Computing Workshops (CLUSTER WORKSHOPS '12)*, pp. 184–191, September 2012.

[53] H. Al-Zurba, T. Landolsi, M. Hassan, and F. Abdelaziz, "On the suitability of using ant colony optimization for routing multimedia content over wireless sensor networks," *International Journal on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks*, vol. 3, no. 2, pp. 15–35, 2011.

[54] W. Cai, X. Jin, Y. Zhang, K. Chen, and R. Wang, "ACO based QoS routing algorithm for wireless sensor networks," in *Ubiquitous Intelligence and Computing*, J. Ma, H. Jin, L. Yang, and J. P. Tsai, Eds., vol. 4159, pp. 419–428, Springer, Berlin, Germany, 2006.

[55] L. Cobo, A. Quintero, and S. Pierre, "Ant-based routing for wireless multimedia sensor networks using multiple QoS metrics," *Computer Networks*, vol. 54, no. 17, pp. 2991–3010, 2010.

[56] I. Politis, M. Tsagkaropoulos, T. Dagiuklas, and S. Kotsopoulos, "Power efficient video multipath transmission over wireless multimedia sensor networks," *Mobile Networks and Applications*, vol. 13, no. 3-4, pp. 274–284, 2008.

[57] L. Shu, Y. Zhang, L. T. Yang, Y. Wang, M. Hauswirth, and N. Xiong, "TPGF: geographic routing in wireless multimedia sensor networks," *Telecommunication Systems*, vol. 44, no. 1-2, pp. 79–95, 2010.

[58] Y. Dong, G. Han, L. Shu, H. Guo, and C. Zhu, "Two-hop geographic multipath routing in duty-cycled wireless sensor networks," in *Wireless Internet*, H. Qian and K. Kang, Eds., vol. 121, pp. 155–166, Springer, Berlin, Germany, 2013.

[59] L. Zhang, M. Hauswirth, L. Shu, Z. Zhou, V. Reynolds, and G. Han, "Multi-priority multi-path selection for video streaming in wireless multimedia sensor networks," in *Ubiquitous Intelligence and Computing*, F. Sandnes, Y. Zhang, C. Rong, L. Yang, and J. Ma, Eds., vol. 5061, pp. 439–452, Springer, Berlin, Germany, 2008.

[60] B.-Y. Li and P.-J. Chuang, "Geographic energy-aware non-interfering multipath routing for multimedia transmission in wireless sensor networks," *Information Sciences*, vol. 249, pp. 24–37, 2013.

[61] S. Medjiah, T. Ahmed, and F. Krief, "AGEM: adaptive greedy-compass energy-aware multipath routing protocol for WMSNs," in *Proceedings of the 7th IEEE Consumer Communications and Networking Conference (CCNC '10)*, pp. 1–6, January 2010.

[62] S. Medjiah, T. Ahmed, and F. Krief, "GEAMS: a geographic energy-aware multipath stream-based routing protocol for WMSNs," in *Proceedings of the Global Information Infrastructure Symposium (GIIS '09)*, pp. 1–8, June 2009.

[63] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM '00)*, pp. 243–254, Boston, Mass, USA, August 2000.

[64] Y. Lan, W. Wenjing, and G. Fuxiang, "A real-time and energy aware QoS routing protocol for multimedia wireless sensor networks," in *Proceedings of the 7th World Congress on Intelligent Control and Automation (WCICA '08)*, pp. 3321–3326, IEEE, Chongqing, China, June 2008.

[65] G. Sun, J. Qi, Z. Zang, and Q. Xu, "A reliable multipath routing algorithm with related congestion control scheme in wireless multimedia sensor networks," in *Proceedings of the 3rd International Conference on Computer Research and Development (ICCRD '11)*, pp. 229–233, March 2011.

[66] M. Xie and Y. Gu, "Multipath routing algorithm for wireless multimedia sensor networks within expected network lifetime," in *Proceedings of the International Conference on Communications and Mobile Computing (CMC '10)*, pp. 284–287, April 2010.

[67] K. Akkaya and M. F. Younis, "Energy and QoS aware routing in wireless sensor networks," *Cluster Computing*, vol. 8, no. 2-3, pp. 179–188, 2005.

[68] S. Poojary and M. M. M. Pai, "Multipath data transfer in wireless multimedia sensor network," in *Proceedings of the 5th International Conference on Broadband Wireless Computing, Communication and Applications (BWCCA '10)*, pp. 379–383, IEEE, Fukuoka, Japan, November 2010.

[69] S. Li, R. Neelisetti, C. Liu, and A. Lim, "Delay-constrained high throughput protocol for multi-path transmission over wireless multimedia sensor networks," in *Proceedings of the 9th IEEE International Symposium on Wireless, Mobile and Multimedia Networks (WoWMoM '08)*, pp. 1–8, IEEE, Newport Beach, Calif, USA, June 2008.

[70] L. Kai and C. Min, "Reliable routing based on energy prediction for wireless multimedia sensor networks," in *Proceedings of the 53rd IEEE Global Communications Conference (GLOBECOM '10)*, pp. 1–5, December 2010.

[71] A. Nayyar, F. Bashir, and R. Ubaid Ur, "Load based energy aware multimedia routing protocol-(LEAR)," in *Proceedings of the 3rd International Conference on Computer Research and Development (ICCRD '11)*, pp. 427–430, 2011.

[72] A. H. Mohajerzadeh, M. H. Yagbmaee, and R. Monsefi, "A QoS based data dissemination protocol for wireless multimedia sensor networks," in *Proceedings of the 3rd International Workshop on Advanced Computational Intelligence (IWACI '10)*, pp. 670–675, August 2010.

[73] G. Padmavathi, D. Shanmugapriya, and M. Kalaivani, "Digital watermarking technique in vehicle identification using wireless sensor networks," in *Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE '10)*, pp. V2-6–V2-10, August 2010.

[74] A. M. Eskicioglu, "Multimedia security in group communications: recent progress in key management, authentication, and watermarking," *Multimedia Systems*, vol. 9, no. 3, pp. 239–248, 2003.

[75] D. Hankerson, A. J. Menezes, and S. Vanstone, "Guide to elliptic curve cryptography," *Computing Reviews*, vol. 46, p. 13, 2005.