Hindawi
Journal of Sensors
Volume 2017, Article ID 4724852, 16 pages
https://doi.org/10.1155/2017/4724852

Review Article

Trust Mechanisms to Secure Routing in Wireless Sensor Networks: Current State of the Research and Open Research Issues

Farruh Ishmanov[1] and Yousaf Bin Zikria[2]

[1]*Department of Electronics and Communication Engineering, Kwangwoon University, 447-1 Wolgye-dong, Nowon-gu, Seoul 139-701, Republic of Korea*
[2]*Department of Information and Communication Engineering, Yeungnam University, 280 Daehak-Ro, Gyeongsan, Gyeongbuk 38541, Republic of Korea*

Correspondence should be addressed to Farruh Ishmanov; farruh@kw.ac.kr

Received 27 September 2016; Accepted 19 February 2017; Published 27 February 2017

Academic Editor: Sara Casciati

Routing is one of the most important operations in wireless sensor networks (WSNs) as it deals with data delivery to base stations. Routing attacks can cripple it easily and degrade the operation of WSNs significantly. Traditional security mechanisms such as cryptography and authentication alone cannot cope with some of the routing attacks as they come from compromised nodes mostly. Recently, trust mechanism is introduced to enhance security and improve cooperation among nodes. In routing, trust mechanism avoids/includes nodes in routing operation based on the estimated trust value. Many trust-based routing protocols are proposed to secure routing, in which they consider different routing attacks. In this research work, our goal is to explore the current research state and identify open research issues by surveying proposed schemes. To achieve our goal we extensively analyze and discuss proposed schemes based on the proposed framework. Moreover, we evaluate proposed schemes based on two important factors, which are energy consumption and attack resiliency. We discuss and present open research issues in the proposed schemes and research field.

1. Introduction

Introduction of sensor nodes which are small, of low cost, and capable of sensing, communicating, and computing leads to the development of wireless sensor networks (WSNs) [1]. These nodes monitor the physical or environmental conditions, such as temperature, sound, vibration, pressure, motion, or pollutants, at different locations [2]. The monitored results are sent to base station, where all the data are collected and sent to user through Internet. A large number of nodes are deployed in open and harsh environments to obtain data from sensor field. Hence, this large number of nodes collaborates with each other to monitor the area and send the monitored result to base station. As capability of the node is limited in terms of sensing area and communication range, there is no choice but cooperating with other nodes in the network. Hence, cooperation of the nodes is vital for the performance of WSNs.

Features of WSNs such as open and harsh environment, open medium, various important applications, and other factors make WSNs susceptible to different attacks [3]. Although traditional security mechanisms such as cryptography and authentication can provide protection at some level, they alone cannot cope with compromised node attacks. Once node is compromised, it can launch attacks according to orders from the outside, which might cripple or control the whole WSNs. For example, malicious node can attract the data from other nodes to it through different means and once it started to receive the data, it can drop all or randomly received data, which significantly degrade performance of the routing protocol. To cope with such kind of nodes is to monitor and detect them. Since there is no central authority in WSNs, nodes should monitor and detect malicious nodes in a distributed manner.

Many solutions are introduced to secure WSNs, including routing. As routing performs data delivery to base station,

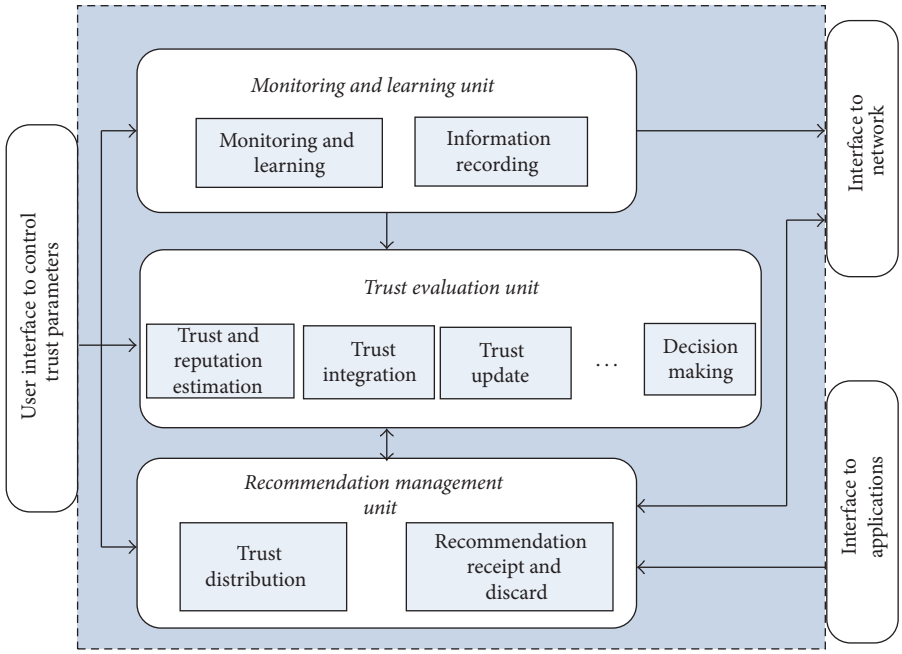

Figure 1: Components of TM and relationships between them.

it is vital protocol for WSNs. Hence, secure routing which is resilient against deliberate packet drops and alterations and disruption acts on routing operation is important. To secure routing, especially against compromised nodes, many solutions are proposed. One of such solutions is trust establishment [3, 4], used in many research fields [5–7]. Trust establishment detects trustworthy and untrustworthy nodes by evaluating them on the basis of their past behavior/performance. It avoids untrustworthy nodes and selects only trustworthy in routing operation. Since trust mechanism is simple and efficient in compromised node detection, a significant research is done to enhance security and improve cooperation in the network.

In this paper, we survey proposed trust mechanisms to secure routing protocols and demonstrate the state of the research field, which is the first paper according to the best of our knowledge. Many overviews and surveys are provided on techniques and solutions to secure routing [1], but there is no research work which overviews proposed trust mechanisms to secure routing and demonstrate the state of the research field. Hence, to demonstrate the state of the trust in routing research field and open research issues, we provided a comprehensive overview of trust mechanisms to secure routing. To achieve our goal and to make reader familiar with the topic, first we discuss and present fundamental issues as such basics of trust mechanism and secure routing. As there are some set of defined attacks against routing protocol, we look for and collect proposed schemes by type of routing attack. Then, we classify existing schemes by routing attack type. In order to analyze and understand proposed schemes more efficiently, we propose framework, which consists of three components. Hence, proposed schemes are presented and discussed based on these three components. Finally, open research issues and recommendations are presented based on the performed comprehensive survey. First, we discuss open research issues in the proposed schemes. Then, we present issues in the research field.

The remainder of this paper is organized as follows. In Section 2, we present background for trust mechanism and secure routing. Section 3 presents proposed framework and overview of the proposed trust mechanisms to secure routing. Open research issues and recommendations are provided in Section 4, and finally, Section 5 concludes the paper.

2. Background

In this section, we discuss briefly fundamentals of secure routing and trust establishment.

2.1. Trust Management. Recently, trust management is used in several applications including routing, data aggregation, access control, and intrusion detection [1]. The term trust management (TM) is used jointly with the terms trust establishment and reputation system and discussed rarely. Trust establishment and reputation system are in fact parts of a TM system, and TM has a wider meaning. In [1], TM is defined as an entity, which addresses managing trust relationships, such as information collection, to make decisions related to trust, assessment of the criteria related to the trust relationship, and observation and reassessment of existing relationships. In the context of routing, TM deals with monitoring neighboring nodes during the transmissions, detecting misbehavior, estimating trust values based on detection results/recommendations, and propagation of trust value/recommendation. So based on the above definition, we can divide TM into three components: monitoring, evaluation, and recommendation management (see Figure 1). Description of each component is as follows.

2.1.1. Monitoring and Learning. Monitor and learn node behavior/performance and provide input to the trust evaluation unit. This is connected to a network interface to collect information about nodes.

2.1.2. Trust Evaluation. This is a central unit of the TM system, which performs estimation and integration of trust and reputation values, trust update, and so on. It provides output to the recommendation management unit.

2.1.3. Recommendation Management. This deals with the distribution and reception of recommendations (trust values). In addition, it provides trust values of nodes for various applications.

We refer to proposed schemes as trust establishment as not all of them include all functions of TM. For example, some schemes do not consider recommendations due to security or energy consumption issues.

2.2. Trust Threshold. It is important factor in the attack detection and performance of trust establishment mechanism. Trust threshold is used to differentiate between malicious and benevolent node. Trust threshold is selected as about half of the maximum trust value in the literature [2–4, 8–11]. Hence, in these articles, defined trust threshold is between 0.4 and 0.8. In [8] the authors suggest that the most intuitive trust threshold is 0.5 when the maximum trust value is 1. Optimal threshold can be estimated by maximizing the false positive alarm rate while keeping false negative alarm rate to minimum [12].

2.3. Trust in Routing. Trust value plays direct role in route selection process. Each node maintains neighbor list along with corresponding trust value. Depending on the routing protocol trust is incorporated in a routing process in different ways to find a trustworthy routing path and avoid a malicious node [12]. Route selection is performed either by source node or by nodes in the routing path (in distributive manner).

2.4. Attacks against Routing. Attacks against routing protocols are studied considerably. Hence, we state only list of attacks rather than discussing them and for descriptions of attacks we refer to [13]. Attacks against routing protocols are as follows [14]:

(i) Grey hole/selective forwarding attack
(ii) Black hole attack
(iii) Sink hole attack
(iv) Spoofed, altered, or replayed routing information
(v) Worm hole attack
(vi) HELLO flood attacks
(vii) Acknowledgement spoofing
(viii) Sybil attacks

Observations show that outcome of these attacks can be one or multiple of the following actions: packet drop, packet alteration, and routing disruption (see Figure 2). Although malicious node might use different techniques to launch a particular attack, generally outcome of the attack matches one of the three of the abovementioned. For example, outcome of black hole, grey hole, acknowledgment spoofing is same, that is, packet drop. Hence, attack avoidance methods based on the outcome of the attack can be easier and efficient rather than based on the attack feature or characteristics.

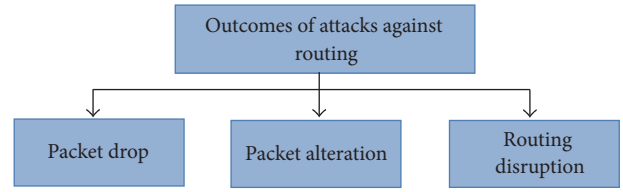

Figure 2: Outcome of the attacks against routing.

2.5. Secure Routing. Routing which is resilient against deliberate packet drops and alterations and disruption acts on routing operation is considered to be a secure routing. Observations on attacks against routing show that attack goals consist of disruption of routing by various means, packet drop, and alteration. Hence, we consider routing as secure if it is prone against such actions.

3. Proposed Trust Mechanisms to Secure Routing

In this section, we discuss proposed trust mechanisms to secure routing. We collected articles based on the attack against which trust mechanism is proposed. In order to find articles based on the specific attack, we made search in google with the following key words: *attack name* + *routing* + *sensor* + *trust*. We use seven types of proposed attacks against routing protocols in [14]. For example, to find papers related to defending against wormhole attack using trust mechanism in routing, we made a search with keywords "*wormhole* + *routing* + *sensor* + *trust*" and we went till tenth web page examining each found paper. Our searches resulted in finding articles related to the following types of attacks:

(i) Greyhole/selective forwarding [15–34]
(ii) Wormhole [35–43]
(iii) Sinkhole [26, 42–50]
(iv) Sybil attacks [51–59]

Since we did not find a significant number of articles for other attacks, we overview articles only for the abovementioned attacks.

Basically any trust-based routing algorithm can be divided into following components (see Figure 3):

(i) Learning
(ii) Trust estimation
(iii) Routing

Learning. Learning component determines if a particular node action is legitimate or illegitimate. In other words, it

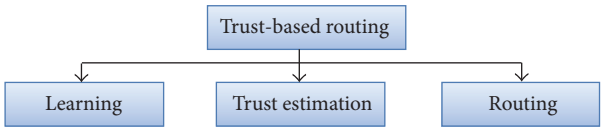

Figure 3: Components of trust-based routing algorithm.

is used to detect the attack. Moreover, it counts the number of legitimate and illegitimate actions and forwards it to trust estimation component.

Trust Estimation. Trust estimation component estimates trust value using certain trust equation based on the number of legitimate and illegitimate actions. It determines if a node is malicious or not using trust threshold and forwards the result to the routing component.

Routing. Routing component includes/excludes the node in routing operation if trust value is above/below trust threshold.

We discuss and analyze proposed trust-based routing protocols based on the above-mentioned three components.

3.1. Trust Mechanisms to Secure Routing against Greyhole/Selective Forwarding Attack

3.1.1. Greyhole/Selective Forwarding Attack. Since limited capability of the nodes requires using multihop communication, nodes act as forwarder also in routing process. Hence, when malicious nodes receive packets to forward them to next hop, they drop instead of forwarding them. The selective forwarding can be in the following forms:

(i) Selectively drop packets from all nodes.

(ii) Selectively drop packets from certain nodes only.

(iii) Drop all incoming packets from any node.

(iv) Drop all incoming packets from certain nodes.

The first and second forms are the most difficult to detect due to conflicting behavior. On the other hand, the last two forms of the attack are easier to detect due to uniform behavior.

3.1.2. Learning Component. Learning component of trust mechanisms for selective forwarding attack deals with detecting deliberate packet droppings. Proposed methods for learning component as follows.

(i) Watchdog-Based Method. Learning component of the proposed trust mechanisms is mostly based on the watchdog mechanism. In fact, out of 17 collected proposed schemes 13 ones [17–20, 22–31] are based on the watchdog mechanism. Watchdog mechanism can be used by nodes which are located on each other's transmission range. In this mechanism, a node sends packets to its neighbor to forward and keeps the packets in the buffer. Once the neighbor starts forwarding, sender overhears forwarder's transmission and compares each received packet with forwarders transmitted packet. If it matches, sender removes the packet from buffer. In this way sender can check if neighbor is forwarding packets. One of the advantages of this mechanism is simplicity, which fulfills the requirements of WSNs. Another advantage is that it does not require any hardware change as promiscuous mode is supported by many network interfaces which is needed to overhear packets. However, there are some issues with watchdog mechanisms. One of the issues is excessive energy consumption due to packet overhearing. This issue is not considered in the proposed schemes. Another issue with watchdog mechanism is detection accuracy which is degraded due to factors stated in [17]. Since output of the learning component is used as input to trust estimation, it has a direct impact on accuracy of estimated trust value. Hence, detection accuracy is important. However, this issue also is rarely considered in the proposed mechanisms except in [22]. The idea in [22] is based on the estimation of normal packet loss, which is loss due to channel quality and MAC layer collision.

(ii) MAC Layer Retransmission Rate-Based Method. One of such trust mechanisms is proposed in [15], which estimates packet drops of its neighbor based on MAC layer retransmission rate. Moreover, it considers packet forwarding cooperativity, which is estimated based on received ACK message from destination through neighbor. Hence, packet forwarding cooperativity of neighbor increases each time when source node receives ACK from destination node through its neighbor. Similarly each node on the routing path maintains packet forwarding cooperativity metric. Advantage of such method is that it eliminates energy consumption due to packet overhearing in watchdog. However, retransmission rate is not affected always by maliciousness; rather it is affected by channel conditions, collisions, and other factors also, which can have impact on detection accuracy. Moreover, malicious node can send ACK message without receiving from destination in order to increase its trust value.

(iii) Watermark Technique-Based Method. Another different method for learning component is proposed in [16], which is based on watermark technique. Watermark technique is used to detect lost packets on destination node. Then, a calculated packet lost rate is compared to normal packet lost rate, which is considered to be 0.01. So, if the calculated packet lost rate is bigger than normal packet lost rate, then it is considered that there is a malicious node on the routing path which launches selective forwarding attack. However, fixing the normal packet loss may lead to wrong detection as it varies depending on channel condition and other factors.

(iv) ACK-Based Method. ACK-based method is proposed in [21]. In this method if a process receives a valid acknowledgment, it means that the sink received the corresponding data message. Hence, upon receiving such an acknowledgment, a process can legitimately increase its confidence on the neighbor to which it previously sent the corresponding data message. Therefore, eventually all honest nodes preferably choose their highly reputed neighbors, and so the data messages tend to follow paths that successfully route data

to the sink. In this case detection is simple; that is, if ACK is received then there is no packet loss; otherwise there is packet drop. However, sending ACK for each packet is not energy efficient. It is known that every packet loss in the network is not due to maliciousness. Hence, it is important to differentiate between packet drop due to maliciousness and other reason.

Black hole attack is considered in [32], which is detected by sending test and data packets through different routes. Hence, if packet is not delivered to sink successfully, then it is assumed that there is black hole attacker in the route. Type of considered attack is not specified in [33]. Rather probability of compromised node based on multiple attacks is considered in learning component. Hence, probability of compromised node is found based on Bayesian network. Moreover, node packet drop is learned by monitoring it in [33]. In [34] idea of establishing a secure trustworthy route based on the present and past node to node interactions is presented. Specifically, it finds and isolates the malicious nodes and a dedicated link is created between every pair of nodes in the selected route with the help of random key predistribution scheme (RKPS) to ensure data delivery from source to destination. However, how the malicious nodes are detected and what kind of attack is considered are not specified in learning component.

Table 1 summarizes learning component methods of proposed trust mechanisms against selective forwarding attack. It includes a brief description of the each method and compares them by presenting their limitation and strength.

3.1.3. Trust Estimation Component. Basically, trust estimation for selective forwarding estimates trust value based on the ratio of number of sent packets to the number of forwarded packets. If estimated trust value of node is under trust threshold then it is considered to be malicious and avoided in routing operation; otherwise it is considered to be legitimate node and involved in routing operation. As in selective forwarding malicious node changes its behavior from forwarding to dropping dynamically, it might be challenging for trust estimation component to detect such node. Basically, there are three major factors which play important role in malicious node detection in trust estimation (see Figure 4):

(i) Correctness of input (number of forwarded and dropped packets)

(ii) Trust estimation equation

(iii) Trust threshold

Input correctness is one of the foremost factors in attack detection which we discussed above in learning component.

Trust equation produces trust value, which determines the node to be malicious or not. There are two components which are usually considered in trust estimation. They are directly associated with trust value and have direct impact on estimated trust value. These two components are past performance/past trust value and recommendation. Consideration of past performance/past trust value in trust estimation for selective forwarding attack is important as it helps to demonstrate node's behavior completely. It might work as inbuilt defense mechanism against selective forwarding attack. For example, in the previous trust estimation period node drops some of the packets and in the current time period it forwards the packets. Combining trust values in these two periods improves accuracy of the trust which helps to detect malicious node. However, when the situation is opposite, it works for the benefit of the malicious node. Hence, proper mechanism is needed when past behavior is considered in trust estimation. Among the proposed schemes only in [9] is past trust value considered as follows [22]:

$$T_{ij}^{X}(t) = \begin{cases} (1-\alpha)\, T_{ij}^{X}(t-\Delta t) + \alpha T_{ij}^{X,\text{direct}}(t), & \text{if } i \text{ and } j \text{ are 1-hop neighbors;} \\ \underset{k \in Ni}{\text{avg}} \left\{ \gamma T_{ij}^{X}(t-\Delta t) + (1-\gamma)\, T_{kj}^{X,\text{recom}}(t) \right\}, & \text{otherwise.} \end{cases} \quad (1)$$

In (1) T_{ij}^{X} is trust value and X indicates a trust component. If node i is a 1-hop neighbor of node j, node i will use its direct observations $T_{ij}^{X,\text{direct}}(t)$ and past experiences $T_{ij}^{X}(t - \Delta t)$; here Δt is a trust update interval. A parameter α ($0 \leq \alpha \leq 1$) is used here to weight these two contributions and to consider trust decay over time. Such α parameter can be used to defend against selective forwarding. For example, when two trust values are combined, heavier weight can be given to lower trust value so that it helps to detect selective forwarding behavior of node in the series of estimation. Although past performance/past trust value plays important role in detecting selective forwarding attacker node, it is not considered in many proposed schemes. Another component used in trust estimation is recommendation. Recommendation is trust value estimated by other nodes on certain node. It is used when direct observations are not enough or impossible. Also it is used to obtain comprehensive trust value. To obtain comprehensive trust value, it is combined with direct observation-based trust value. In this case, it helps with colluding attacks and demonstrating more real behavior of node. Some of the proposed schemes consider recommendation component in trust estimation. In fact, out of 17 proposed schemes 8 ones [19, 21–23, 25, 33, 34] consider recommendation component. Although recommendation component has benefits, there are 2 major issues related with recommendation: energy consumption overhead and blackmouthing attack. In order to consider recommendation in trust estimation, nodes need to transmit and receive it, which requires high energy consumption. Another issue is dishonest recommendations by malicious nodes, which has significant

Table 1: Learning component methods of trust mechanisms against selective forwarding attack.

Learning component method	Description	Limitation	Strength
Watchdog-based method	Overhearing neighbor transmission and checking if it is transmitting the packets	High energy consumption due to packet overhearing	Simple and more accurate detection compared to other methods
MAC layer retransmission-based method	According RTS/CTS mechanism, when a receiver receives packet, it sends back ACK message to a sender. If the sender does not receive ACK it and retransmits the packet	Detection accuracy is low due to no differentiation between retransmission due to collision or other factor and deliberate packet drop	Simple and no specific algorithm or method is needed
ACK-based method	Receiving ACK message from destination through neighbor indicates that packet is received	High energy consumption due to sending and receiving ACK messages for each packet	Collusion attacks are difficult to launch

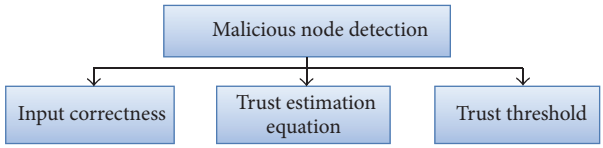

Figure 4: Factors affecting malicious node detection (in selective forwarding) in trust estimation component.

impact on estimated trust value. The proposed 8 schemes consider different mechanisms to cope with black-mouthing attack. However, energy consumption due to recommendation exchange is rarely considered.

Once trust value is obtained, mostly trust threshold is used to detect malicious and legitimate node. In fact, out of 17 collected proposed schemes 13 ones [16–18, 20–28, 30, 33, 34] use trust threshold to differentiate between malicious and legitimate node. It is important metric to detect malicious node and avoid false accusation. Optimal trust threshold maximizes malicious node detection and minimizes false accusations. However, proposed schemes do not discuss optimal threshold. In fact, only in [22] is it found as 0.7 when maximum trust value is 1. It is important to note that it depends on the trust estimation scheme. Hence, it is important to define optimal trust threshold when trust estimation scheme is proposed. Some of the trust mechanisms [28] propose using dynamic trust threshold rather than fixed one, which is defined as half of the average trust values of the nodes in the network. Trust schemes which do not use trust threshold use different approaches to avoid malicious nodes. For example, in [15, 20] malicious node detection depends on certain criteria rather trust threshold.

3.1.4. Routing Component. This component defines routing algorithm, which uses trust value with other metrics to select route to send data to destination. Many of the proposed routing algorithms [15, 17, 20, 27, 29–31] are based on *geographic routing*. On the other hand, some of the proposed trust mechanisms [21–23, 28] *do not consider* routing algorithm. *Various* routing algorithms which consider different techniques and metrics are also introduced [18, 19, 24–26, 32–34]. For the routing algorithms which are based on geographic routing combine trust information with location information for routing. Some of the routing algorithms [15, 17, 20] are based on greedy perimeter stateless routing while others consider only distance metric without specifying any technique [30, 31]. Some of the routing algorithms [17] use multipath routing technique. In [30] authors focus on different ways to integrate trust information in geographic routing. They introduce weighted routing cost function to perform trust- and location-aware routing. When a node has data to send to the base station, it creates a transaction made up of a specific number of packets. The number of hops to the base station and the sending node's trust is considered metric in [18]. When node has data to send, transaction is created and routing path is established based on the defined metric. Each packet in the transaction uses this chosen path. After each transaction, a trust reporting phase begins, in which nodes compute trust values for the nodes in the path of the transaction. In [19], in order to send a packet to destination node, first source node finds trusted nodes among the neighbors by sending recommendation request. Then, it sends route request to trusted node; if trusted nodes have route to destination node, they will reply to source node; otherwise they will repeat the initial action of source node. By this way, destination node receives the route request message and it replies with route reply to source node. Upon receiving the route reply/replies source node selects most trusted path. In [28] nodes called monitor nodes are used for each area. These nodes are responsible for monitoring neighborhood and providing information about trustworthy nodes. When source node has data to send, it communicates with monitor node in its area and obtains ID of trustworthy forwarder. Upon receiving ID of the forwarder it sends the data to the forwarder. Monitor node selects forwarder based on trust and power. In turn when forwarder receives data from source node, it requests monitor node in its area about possible forwarder ID. In this way, data reached to destination. Secure routing algorithm for inquiry-based WSN is proposed in [26]. So in this scheme, first sink node requests data. Then, it is broadcasted till it reaches the source node. Then, source node broadcasts the report which is broadcasted by intermediate nodes until it reaches the sink node. Finally, when a confirmation packet is sent to the source node by the sink which informs that it is ready to receive data from source, simultaneously forwarding the

packet from sink, forwarding paths with different trust levels are created. Two types of routing are defined in [32]: detection and data route. In detection route routing works without data packets so that it can identify the attack behavior and then mark the black hole location. The data routing is sending node data to sink. The difference between common routing protocol in WSNs and proposed one is considering trust of the neighbor nodes to select next hop. Routing in [33] is based on AODV routing protocol. It discovers and selects routes on the basis of maximum utility with incurring additional cost in overhead. However, as authors claim overhead is due to energy consideration in routing. Routing component in [34] is based on trust aware secure routing framework. The idea of the routing is first detected and isolates the malicious nodes using trust establishment and then creates dedicated between transmitter and receiver. This dedicated link is created with the help of composite RKPS.

3.2. Trust Mechanisms to Secure Routing against Wormhole Attack

3.2.1. Wormhole Attack. As the name of the attack suggests, two distant malicious nodes create a wormhole through which packets are "tunneled" from one part of the network to another part and replayed there. Since tunneled distances longer than the normal wireless transmission range of a single hop, the tunneled packet can be delivered with minimum delay, which makes the path through malicious node attractive to traffic. Consequences of this attack can be various depending on the attacker goal. For example, after traffic attraction malicious node can drop all/selective packets or they aim to disrupt routing procedure by replying routing control/data packets in different parts of the network.

Proposed mechanisms are different in terms of detection and avoidance of wormhole attack. As attack involves two nodes and complicated operations, detection techniques and methods are also different. Below we discuss their component by component of the proposed mechanisms.

3.2.2. Learning Component. In this component of the proposed mechanisms different methods and techniques are introduced to detect and avoid the wormhole attack. Although most of the proposed mechanisms are based on detection method, some of the proposed mechanisms use avoidance method [36]. Hence, in [36] authors do not consider detection method; rather avoidance method in trust estimation component is considered. Proposed detection methods are mostly based on the some *certain feature of wormhole attack*. They are as follows.

(i) Maximum Transmission Range-Based Method. Based on the closed type of wormhole attack authors proposed [35] detection mechanism, in which if maximum transmission range of the neighborhood node is greater than maximum transmission range in the network than node is suspected as malicious node. When node receives HELLO message from source node, it responds with appending HELLO message with presented received time and reply. Upon receiving source node calculates distance between itself and destination. If distance is greater than sender node (neighbor of source node) maximum transmission capacity then wormhole is suspected and ignores suspicious neighbor and selects discovering an alternate route. Key point here is to calculate the distance by received time of HELLO message from neighbor. However, intelligent malicious node may reply with wrong time to trick the source node. Moreover, in order for the mechanism to work tight clock synchronization is required, which may not be feasible always.

(ii) Packet Forwarding Time-Based Method. It is assumed that malicious node takes longer time to forward packet to another colluding node compared to packet forwarding time between legitimate one-hop neighbors [36]. Although this idea holds true, it assumes that distance between nodes does not differ much, which may not be always true. For example, when distance between two legitimate nodes is longer, they can be considered malicious wrongly. Hence, it is important to define how long packet forwarding time is long in this mechanism.

(iii) HELLO Packet Received Time-Based Method. In [37] similar idea based mechanism to the above-mentioned scheme is proposed, which considers the neighboring node's HELLO packet received time. If packet is received in time, then neighbor node is considered to be legitimate. Calculation details of packet receiving time are not stated.

(iv) Routing Paths Checking-Based Method. All existing routing paths to destination are compared to detect wormhole. If among neighbors only one has very short path and others have considerably long paths then it determines that the corresponding one-hop neighbor nodes are wormhole nodes with great probability.

(v) Packet Modification-Based Method. Another detection method is proposed in [42], which works based on the checking the modification of Dynamic Source Routing (DSR) [60] packet. Assuming that in wormhole attack packets received by a malicious node are not forwarded according to routing path but rather they are modified and sent to the colluding node, in the proposed scheme integrity of DSR packets is monitored closely. Promiscuous mode is used to check if the packet is modified. Although proposed method is simple, it has limitations such as routing dependency and energy consumption overhead in promiscuous mode. Moreover, using only one sign of wormhole attack to detect it may not lead always to accurate detection.

(vi) Two-Hop Neighbor-Based Method. List of two-hop neighbors is maintained in each node to avoid wormhole attack in [46]. Node monitors its one-hop neighbor during the transmission whether it is forwarding to next neighbor or to colluding malicious node. Although this method can avoid wormhole attack, it cannot avoid all types of wormhole attack.

Some comprehensive methods such as *statistic* and *genetic algorithm* based methods are as follows.

(vii) Unsupervised Genetic Algorithm Based Method. The idea is to analyze temporal and spatial inconsistencies in routing paths using unsupervised genetic algorithm [37]. If

the estimated inconsistency is higher than a certain threshold then it is assumed that there is attack and attack's location is determined. Advantage of such schemes is that they provide accurate inference about attack as they involve deeply scientific analytical methods. However, a limitation of such scheme is that it works well in stationary environment rather than mobile one as key idea of the inferring the attack in the scheme is based on the inconsistency of the routing paths.

(viii) Statistical Method-Based Method. Although certain method is not proposed in [38], authors refer to using localization information and route analysis for messages coming from the same area. Specifically, authors refer to use of statistical process of network data to detect wormholes.

3.2.3. Trust Estimation Component. Trust estimation methods against wormhole attack consider various factors and equations to estimate trust. Detection factors of wormhole attack are based on the signs of it. Considered factors to estimate trust are as follows:

(i) Packet forwarding behavior and estimated sign of wormhole attack [35]

(ii) Bandwidth requirement of the particular route and data rate of the transceiver at node [36]

(iii) Previous reputation value and level of inconsistencies in routing paths [37]

(iv) Spatial and temporal changes in routing path [38]

(v) Packet forwarding time [39]

(vi) Packet forwarding behavior and HELLO packet received time [40]

(vii) Packet forwarding behavior and route length [41]

(viii) Packet forwarding behavior and packet integrity [42]

Although trust estimation equation is central to proposed scheme some of the schemes do not consider it [35, 38, 42]. Proposed trust estimation equations are diverse. Unique trust estimation approach is introduced in [35]. End-to-end routing metric increases with route length, which avoids wormhole attack by helping to choose the route which has a maximum routing metric. Reputation (trust) of any node is increased on each successful routing response from the sink by the ratio of the bandwidth requirement of the particular route (its data rate request carried in a routing header) to the data rate of the transceiver at node. A contribution to the value of the end-to-end reputation from any individual node is logarithmic which makes the reputation algorithm towards the use of previously explored nodes wherever possible. Reputation (trust) level of node in [38] is estimated based on the previous reputation value and level of inconsistencies in the node link of routing path. If the previous reputation is above the threshold and the node starts misbehaving, its reputation will decrease rapidly. On the other hand, if the reputation is lower than the established threshold and the node starts behaving properly, it will need to behave properly for some time until it reaches the threshold. In [36], direct trust is estimated based on the number of correct and incorrect packet forwarding processes. Then, indirect trust is combined with direct trust to obtain final trust. If estimated trust value is lower than trust threshold, node is not believed and not selected for routing operation. In [40] authors consider packet forwarding behavior and HELLO packet received time to estimate trust. First ratio of number of good (packet forwarding/received HELLO packet in time) to bad behaviors (packet drop/received HELLO packet not in time) is estimated. Then, estimated ratios for packet forwarding and HELLO packet received time are combined to obtain final trust value. In [41] trust is estimated based on the packet forwarding behavior and route length to destination. Trust equation is designed in such a way that the trust value increases slowly but decreases rapidly. Anomaly threshold of the route length difference is defined to avoid wormhole attack. First, source node finds the shortest routing path among existing routes to destination. Next, it finds the second shortest routing path through the node which is selected to send packet. If the difference between shortest path and second shortest routing path through selected node is bigger than anomaly threshold of the route length difference, then it is assumed that there is wormhole and different weights are assigned in trust estimation so that trust is decreased rapidly. In [42], trust is estimated simply by multiplying two factors: packet forwarding behavior and estimated sign of wormhole attack.

3.2.4. Routing Component. Generally routing algorithms avoid wormhole nodes in path selection using trust values. Various routing algorithms are proposed in which they modify existing routing protocols by integrating trust. In [35] trust-based ad hoc on-demand distance vector (AODV) [61] routing is proposed, in which when node receives AODV HELLO packet, it replies appending HELLO packet with present received time. This is to detect wormhole attack. Route is selected based on trust and other parameters. Remaining routing operations are identical to AODV protocol. Simulation results show that proposed routing algorithm outperforms AODV in terms of packet delivery ratio and end-to-end delay in the presence of wormhole attack. However, evaluation in terms of energy consumption is not considered. Trust-based DSR is proposed in [42]. Cost link in DSR is changed to trust level of the node. In case the status of the link end node is classified as a wormhole, the cost of that link is set to infinity. Packets are forwarded according to the list in source route header. If forwarder detects malicious node in the list, packet is dropped and ROUTE ERROR packet is sent to source node. According to performance evaluation proposed routing algorithm outperforms greedy perimeter stateless routing (GPSR) [55] and DSR in terms of packet loss, throughput, and latency. In this work also evaluation in terms of energy consumption is not considered. Moreover, energy is not considered as metric in routing. General type of routing is proposed in [36]. According to this routing algorithm the sink chooses the route with the lowest end-to-end aggregate. Routing metric of link is determined based on the ratio of the bandwidth requirement of the particular route (its data rate request carried in a routing header) to the data rate of the transceiver at node. The basic idea of route

selection mechanism is to select longer and older routes to avoid wormhole attack. Energy considerations are skipped in this work too. In [37, 43] routing algorithm is not considered. In [38] authors refer to use of cluster based routing, but they do not provide any details about it. Another AODV-based routing algorithm is proposed in [39]. According to proposed algorithm when node receives RREQ or RREP, it checks trust value of the sender. If it is below threshold, it discards RREQ/RREP; otherwise it forwards RREQ. The remaining operation of the algorithm is similar to AODV's operation. The trust is used in [40] to select multipoint relaying (MPR) nodes in Optimized Link State Routing (OLSR) [62]. That is, only nodes with high trust values can be MPR node. MPR nodes perform two tasks: (1) forwarding selector's packets; (2) broadcasting its selector list. The remaining operations of the routing algorithm are identical with OLSR. Multipath trust-based routing is proposed in [41]. Multipath routes are constructed according to proposed mechanism and trust values are used when paths are selected to construct the routes. Authors compare proposed routing algorithm with AODV, single signature SAODV [63] (SS-SADOV), and double signature SAODV (DS-SADOV) [63] in terms of packet delivery rate in the presence of wormhole attack, in which proposed algorithm outperforms other routing algorithms.

Our observations on proposed routing algorithms show that none of the proposed algorithms consider energy issues despite their high importance in WSNs.

3.3. Trust Mechanisms to Secure Routing against Sinkhole Attack

3.3.1. Sinkhole Attacks. In this attack, first malicious node attracts traffic by spoofed, altered, or replayed routing information. Then, it can selectively forward the packets or tamper them before forwarding [14]. Below we discuss proposed trust mechanisms to secure routing against sinkhole attack component by component.

3.3.2. Learning Component. Detection of sinkhole attack can be two parts: (1) detection of spoofed, altered, or replayed routing information; (2) detection of packet drop or tamper. Our analysis results on proposed trust mechanisms show that detection methods mostly rely on watchdog-based mechanism. Interestingly, many of the proposed trust mechanisms do not consider detection method; rather authors assume that there exists some detection method. Specifically, proposed mechanisms in terms of detection methods are as follows.

(i) Watchdog-Based Methods [26, 42, 44–46, 49]. As we discussed above, node can overhear its neighbor transmissions, in which it buffers all transmitted packets to its neighbor. Then, when neighbor starts to forward packets, it catches and compares each forwarded packet with buffered packet. By this way, it checks if neighbor is forwarding the packets. Hence, in order to detect sinkhole attack, packet drop characteristic of sinkhole is considered.

(ii) Energy Hole and Promiscuous Mode Monitoring Method. One of the characteristics of sinkhole attack is to attract as much as traffic which implies that nodes around malicious node will consume more energy compared to other nodes [49]. Based on this implication, authors compare average energy consumption rates in each zone to find energy hole. Once energy hole is found, to detect selective forwarding part of sinkhole attack promiscuous mode monitoring is used. To save energy promiscuous mode is used only when energy hole is detected.

(iii) Neighbor List and Signal Rule [53]. Assuming that a malicious node convinces its neighbors as the nearest path to base station using high transmission power, nodes use neighbor's list and predefined signal rule to check if a packet is originated from a far located node.

(iv) Forwarded Sequence Interval [48]. Malicious node can replay routing information to attract traffic. To detect such action, node compares stored table of smaller node ID of a source node, forwarded sequence interval [a, b] with the broadcast messages from the base station about data delivery.

(v) Number of Received ACK from Sink [50]. Taking into account selective forwarding feature of sinkhole attack, selective forwarding behavior in the routing path through particular neighbor is determined based the number of received ACK from sink for sent messages.

As shown above, proposed and considered detection mechanisms are based on the some feature of sinkhole attack. None of the detection mechanisms consider complete feature of sinkhole attack, which has impact on detection performance. As many of them rely on promiscuous mode monitoring, which consumes high energy, this issue also is not considered.

3.3.3. Trust Estimation Component. Trust estimation methods against sinkhole attack consider various factors and equations to estimate trust. Factors depend on the considered feature of sinkhole attack to detect. Mostly considered factors are packet forwarding and sinkhole attack behavior. Considered factors to estimate trust are as follows.

(i) Packet Forwarding Behavior [29]. It is considered factor to estimate trust value. Unique trust estimation is proposed, in which position and distribution of malicious nodes are considered in trust estimation. As intelligent malicious nodes position themselves near to sink to have more chance to receive more traffic and to drop, the closer the node to the sink is the more severe the measurements are taken for packet drop. Moreover, unstable behavior also is considered in trust estimation. The more unstable the behavior of the node, the more severe the measurements that are taken into account.

(ii) Packet Forwarding Behavior and Packet Integrity [42]. They are considered factors to estimate trust value. Trust estimation is simple. Defined two factors are simply multiplied to estimate trust value.

Trust estimation is not considered in [43].

(iii) Packet Forwarding Behavior [44]. It is considered factor to estimate trust value. First trust is estimated based on the

number of forwarded and dropped packets. Then, recommendations are integrated to the trust value. Finally, to obtain final trust value, estimated trust value in previous time period combined with current one. In recommendation collection bad-mouthing attack is not considered, which may degrade accuracy of estimated trust value significantly.

(iv) Number of Packets Reached at Destination [45]. Although trust estimation equation is not considered, two types of trust are introduced: route and node trust. Both of these trusts are associated with each other. Node trust is estimated based on the difference between route trust value and the observed trust value. Route trust is estimated based on the number of packets received at destination and forwarded by the node under consideration.

(v) Packet Forwarding Behavior and Packet Integrity [46]. They are considered factors to estimate trust value. Although factors are introduced to estimate trust, trust equation is not proposed.

(vi) Packet Forwarding Behavior and Packet Integrity [47]. They are considered as in [46] to estimate trust value. In this proposed mechanism also trust estimation equation is not considered.

(vii) Delivery Ratio and Detected Loop [48]. They are considered to estimate trust value. Two types of trust are maintained: one for the delivery ratio and another for routing loop. Previous trust value is combined with current one.

(viii) Numbers of Packets Forwarded and Number of Packets Forwarded without Tampering [47]. They are considered factors to estimate trust value. Trust is estimated simply by adding these factors, which are multiplied by defined weight values. As in [54] recommendation and previous estimated trust value are combined with currently estimated trust value to obtain final trust value. In this work also, bad-mouthing attack is not considered.

(ix) Number of Sent Packets by Source and Number of Received Packets at Sink Node [50]. They are considered factors to estimate trust value. Trust is estimated based on the number packets sent by source node and received at sink node. Hence, it is based on the route trust rather than individual node. Way of obtaining the number of received packets at the sink node is not discussed.

Our observations on the proposed trust estimation method conclude that in any of the proposed trust estimation methods consider accuracy of estimated trust value.

3.3.4. Routing Component. Proposed trust-based routing algorithms against sinkhole are as follows.

In [26] query-based routing is proposed, in which first sink nodes queries network about sensor data that will be broadcasted until query reaches the source node. Once source node receives the query, it broadcasts the sensor data. Each node that receives the packet forwards it to its neighbors until it is received by the sink. Each intermediate node which receives the packet creates a record, in which trust value of the path up to current node, the source node ID, the sender node ID, and the number of covered hops are kept. In this routing table all the possible routes are determined by considering the trust values of the paths between the sink and the source node sensing the event. A sink sends confirmation to the source node in which it informs that it is ready to receive data from source. Different trust level paths are constructed based on the temporary routing table which is created during the query packet forwarding. Although proposed routing protocol is query-based, route finding process is general which can be applied to any routing protocol. However, control of broadcast messages is not considered which causes message overhead. Moreover, energy metric in routing is not considered.

Routing algorithm is not considered in [42–44].

AODV-based routing is proposed in [45], which is called SAODV. A significant difference between AODV and SAODV is that route selection criterion in SAODV is trust value. Moreover, unlike AODV in SAODV route trust along with node trust is maintained. Each node keeps track of the number of packets it has forwarded through a certain route. Destination sends R_ACK packets to S periodically. The R_ACK is received packet report. It is readable by all the nodes on the route. Each intermediate node on the reverse route can estimate its route trust based on the R_ACK packets. When source receives RREP packets in response to its RREQ packet to destination, the route selection criterion is dependent on node trust on the immediate downstream neighbor N that recommended the route which has trusted route.

The strength of the proposed routing protocol is that it considers route trust along with node trust which makes it more resilient to attack. However, energy consumption is not considered in this proposed routing too. As route is selected solely based on trust value, energy consumption of the selected route might be high.

DSR-based routing is proposed in [46], which is called S-DSR. Packets are forwarded according to the list in the source route header. If forwarder detects malicious node in the list, packet is dropped and ROUTE ERROR packet is sent to source node. According to performance evaluation proposed routing algorithm outperforms DSR in terms of packet delivery ratio. In this work also energy consumption is not considered.

Geographic routing which is called Trust-Based Energy Aware Greedy Perimeter Stateless Routing (TEGPSR) is proposed in [44]. Considered metrics to select route are trust, distance, and energy. To consider energy efficiency, nodes periodically broadcast HELLO packet, which contains location information of node, rate of energy consumption, and fraction of energy consumption. The adjacent neighbor which has minimum energy level requirement and least distance to a particular destination for forwarding the packet is selected from node's neighborhood table. The merit of the routing is that it considers energy and trust together, which improve performance of the routing in terms of energy consumption and security. On the other hand, being geographic-based routing limits its implementation to other scenarios.

Kind of universal routing framework is proposed in [48]. It considers trust and energy in route selection. Energy watcher component estimates energy cost for its neighborhood table and its own energy cost for nodes as a next hop node. It also estimates average energy cost of successfully delivering a unit-sized data packet from N to the base station, with b as N's next hop node being responsible for the remaining route. Hence, energy watcher component helps in route selection. Details of route selection and routing process are not discussed. Moreover, performance evaluation is not provided except a little.

Another geographic routing is introduced in [49], which is titled as BT-GPSR. BT-GPSR operates in similar manner to GPRS except it considers trust and distance in route selection. Limitation of this routing algorithm is that it does not consider energy like many routing algorithms. Comparison of performance with other routing algorithms would give more insight into performance of the proposed routing algorithm. Unfortunately, in many routing algorithms such evaluations are not provided including in this proposed algorithm.

Trust is integrated in a gradient based routing algorithm in [50]. It assumes that energy level of the neighbor and hop-count from neighbor to sink are known to each node. Hence, when a node needs to send a message it finds lowest neighbor node (optimal in terms of trust, energy, and hop-count) and sends the message to this node. If a node is located at a local minimum, it sends the message directly to the sink/base station.

3.4. Trust Mechanisms to Secure Routing against Sybil Attack

3.4.1. Sybil Attacks. In this attack, attacker uses multiple identities and advertises it to the rest of the network. As a result of this attack, neighborhood detection, topology maintenance, and most importantly route formation can be crippled which leads to a significant degradation of routing protocol performance.

3.4.2. Learning Component. Trust-based Sybil attack detection method is proposed in [48]. The idea is based on the node resource utilization. A master (observer) node collects the identifier of all nodes and send them data. Through communications it identifies the nodes with maximum packet drop, which is suspected as Sybil node. Then, it calculates their resource utilization from which it extracts the standard value. The deviation from the standard value for suspected node is used to categorize the node as trust, distrust, or enemy. In the learning component of the proposed scheme in [52], nodes consider consistency, normality, and battery level to detect attack. Behavior of Sybil attack node is defined as providing wrong sensor data (consistency), less participation in detection process (normality), and low battery level. However how to obtain information normality and battery level is not discussed. Moreover, defined factors to detect Sybil attack are not directly related. Trust in FIGA is derived through the number of interactions, which a node has with another node. Dealing with number of interactions with neighbors and recommendations from neighbors is task in learning component of the scheme [50]. However, detection of Sybil attack is not discussed in [53]. In [54] detection of routing loops and delivery ratio is considered in learning component. Moreover, energy measurements are performed in this component. To detect loops, it checks a received data packet in record table. If it is already in that record table, it will drop the packet and next hop node's trust level. Delivered packets to base stations are determined based on the broadcast messages from the base station about data delivery. It computes the ratio of the number of successfully delivered packets which are forwarded by this node to the number of those forwarded data packets. Energy computations are about energy consumption to next hop neighbor and next hop neighbor's energy consumption to base station, which are used for routing selection decision. Unlike many schemes, in this scheme promiscuous mode is not used to detect packet drops. This has both advantage and disadvantage. The advantage is that it is free of high energy consumption of promiscuous mode. On the other hand, the disadvantage is that it relies on broadcast ACK from base station about data delivery, which might not be feasible always. Moreover, there can be ACK lost cases, which has direct impact on trust value accuracy. In [55] quite similar work to [54] is proposed. In this work learning component method aims to detect packet forwarding and routing loop. Packet forwarding detection is based on watchdog mechanism and loop detection method is same as that in [54]. Although in [56] trust-based routing algorithm is proposed, it does not describe how to derive trust values for nodes. Rather authors focus on deploying genetic algorithm into Low Energy Adaptive Clustering Hierarchy-Energy (LEACH) [64] to avoid Sybil attack. A sensor value and packet forwarding behavior checking is the task of learning component of the proposed scheme in [57]. The checking is based on the watchdog mechanism. Although defined metrics do not have direct relation to Sybil attack, evaluation results show that proposed scheme resists Sybil attack. The advantage of the proposed method is consideration of the energy consumption in watchdog mechanism. According to our best knowledge this is the first scheme, which considers energy consumption in watchdog mechanism. Energy consumption is optimized considering frequency and location of watchdog. Moreover, tradeoff is shown between energy consumption in watchdog and security in performance evaluations. Several factors are considered in learning component in the proposed scheme [55]. Specifically, number of sent and forwarded packets, last claimed location, and average delay in relaying messages are considered factors. The number of forwarded packets and average delay in relaying the messages are determined using watchdog mechanism. For the location verification, authors do not define any method. Based on the defined factors some metrics are derived such as forwarding success ratio, forwarding fairness ratio, a consistency score based on the variance of neighbor N's claimed locations, and forwarding performance of the neighbor in terms of the maximum delay. Hence, based on these metrics reputation is estimated. Advantage of the proposed scheme is that it considers the factors comprehensively to estimate reputation, which can improve the security. On the other hand, considering such factors without energy consumption consideration makes the proposed scheme less attractive to WSNs. Similar to

many other proposed schemes to detect or avoid Sybil attack, unrelated feature to Sybil attack is considered in learning component [56]. Specifically, authors consider consistency of provided sensor data. An outlier is detected for provided sensor data by nodes using self-organizing map, which considers temporal and spatial features. Hence, if a node provides sensor data which differs significantly with neighbor nodes sensor data then it is assumed that node is malicious. Advantage of the proposed scheme is it employs robust statistical method which can detect outliers in a given data. However, it is unacceptable that considered factor to avoid Sybil attack is not related to Sybil attack. Moreover, energy consumption is not considered in the proposed scheme.

Our observations on proposed trust mechanisms to detect or avoid Sybil attack demonstrate that most of the proposed mechanisms consider unrelated feature to Sybil attack to detect or avoid the attack. Moreover, except in [58] energy consumption issues are not taken into account in other proposed works.

3.4.3. Trust Estimation Component. Trust is estimated based on the factors defined in learning component. Proposed trust estimation methods follow generally accepted way of trust estimation, which is defined by taking the ratio of number of good actions to the bad actions in general. They are different in terms of considered factors to estimate trust. Moreover, some of the trust estimation methods consider previous trust value [54, 55, 58] and some do not consider it. Considering previous trust value in trust estimation can demonstrate node behavior accurately. However, it requires additional memory space to store the trust value. Most of the proposed trust estimation methods rely on trust threshold to avoid malicious node. However, selection method or threshold value is not discussed in these proposed trust estimation methods. Some of the proposed mechanisms do not consider trust estimation equation [51, 53, 56]. Rather, they focus on routing description [48] or integration of trust into routing using different techniques [53, 56]. Our observations on proposed trust estimation equations show that none of the proposed method considers additional measures or components, which improves detection or avoidance of Sybil attack. Rather, considered factors to estimate trust do not have direct relation to Sybil attack feature.

3.4.4. Routing Component. Most of the proposed schemes do not consider routing algorithm. In fact, routing is considered only in [54–56, 58]. A distributed kind of routing is proposed in [54], in which route selection process is performed in a distributive manner. A node selects neighbor node based on the trust value and energy cost of delivery of packet to send a packet to base station. Base station broadcasts message about lost packets. Whenever a node receives such a broadcast message from the base station, it knows that the most recent period has ended and a new period has just started. Advantage of such routing protocol is that it is general which can be applied to any scenario with a little modification. Moreover, energy consideration makes it energy efficient. However, energy cost of packet delivery is reported by each node. This might be exploited by malicious nodes to attract more traffic. Although such attack can be detected finally, but nature of the proposed scheme it takes a long time to detect such exploit. Very similar work to [54] is proposed in [56]. Routing considers energy and trust value to select node to send the packet to base station. Also, lost packets are reported by base station to all nodes in the network. LEACH protocol based routing protocol using genetic algorithm is proposed in [56]. As LEACH is cluster based structure, routing is based on the clusters. To select the node to send the packet to base station genetic algorithm is used with node-energy, node-trust value, and node-distance. Genetic algorithm uses fitness function to which node behavior should fit. If it does not fit then it is considered to be Sybil node which is excluded from routing operations. Moreover, genetic algorithm is used to form clusters. As paper focuses on describing application of genetic algorithm in node selection and cluster forming, routing is not described in detail. For example, how packet is routed to base station is not elaborated. A flexible routing protocol is proposed in [58], which is called Secure Implicit Geographic Forwarding (SIGF). The proposed routing can be configured to one of the three modes depending on the security situation. In the first state, it uses nondeterminism and candidate sampling to achieve high packet delivery ratios probabilistically. In the second mode, it maintains a reputation of the neighbors that are maintained and neighbors are selected based the reputation value. In the last mode, it uses cryptographic mechanisms along with reputation mechanism. Flexibility and resource consideration is merit of the proposed scheme. However, in route selection nodes are selected randomly among high reputable nodes; selected path might not be energy efficient always.

In Table 2, we present a summary of the proposed trust-based routing protocols by attack. In the first column, proposed methods for learning component are presented. In the next column, proposed methods for trust estimation components are described. Finally, in the last column proposed routing algorithms for routing component are presented.

4. Open Research Issues and Recommendations

In this section, we briefly discuss open research issues in the proposed schemes and research field in general. Open research issues in the proposed schemes are as follows.

4.1. Selective Forwarding Attack. As we discussed in Section 3.1 the fact that attack detection methods are based on watchdog mechanism. Watchdog mechanism has a number of issues which are not addressed in the proposed schemes mostly. One of the issues is high energy consumption due to transmission overhearing in watchdog mechanism. To decrease energy consumption in watchdog operation transmission overhearing can be periodic overhearing or frequency of overhearing can be defined based on the detection criteria or priority. Lack of consideration about low duty cycle of the nodes is another issue in the watchdog-based detection schemes. Proposed schemes assume that nodes continuously overhear transmissions and detect number of forwarded and

Table 2: Summary of the proposed trust-based routing protocols.

Attack	Component		
	Learning	Trust estimation	Routing
Selective forwarding	Most of the methods are based on the watchdog mechanism.	Basically trust is estimated based on the number of dropped and forwarded packets. Some proposed schemes propose combining previous trust value and recommendations with current estimated trust.	Many of the secure routing schemes against selective forwarding are based on geographic routing. Moreover, various other routing algorithms are proposed. Basically they consider trust value along with other metrics to select route to send the packet.
Wormhole	Detection methods are based on the different feature of the wormhole attack. Checking the transmission range, routing path, and two-hop neighborhood can be examples for wormhole feature based detection. Moreover, detection methods consider packet forwarding behavior.	Most of the schemes estimate trust is estimated based on the on the number of dropped and forwarded packets and estimated sign of wormhole attack.	Generally routing algorithms avoided wormhole nodes in path selection using trust values. Various routing algorithms are proposed in which they modify existing routing protocols by integrating trust. For example, AODV-, DSR-, and OLSR-based routing protocols are proposed.
Sinkhole	Proposed detection methods consider packet forwarding behavior and some signs of sinkhole attack such as energy hole, neighbor list. Packet forwarding behavior is checked using watchdog mechanism.	Mostly trust is estimated based on the number of dropped and forwarded packets.	Some proposed schemes do not consider routing algorithm. The remaining schemes consider AODV, DSR, and geographic routing algorithms. Trust is integrated in these routing protocols in a different way.
Sybil	Detection methods consider different factors which are not related to Sybil attack directly. For example, correctness of sensor value, packet forwarding behavior, battery level, and others are considered factors.	Although some proposed schemes do not consider trust estimation equation, basically trust estimation equations consider factors in the learning component to estimate trust value.	Many of the proposed schemes do not consider routing algorithm. The remaining ones are various protocols such as LEACH-based, geographic, and distributed ones.

dropped packets, which is feasible. Transmissions overhear scheduling which is based on the duty cycle of the node and can be one of the solutions for this problem. Moreover, it can decrease also energy consumption of the watchdog mechanism. Last issue of the watchdog mechanism is that it does not differentiate between packet drop due to not maliciousness and some factors like channel condition, collision, and so forth. Weight factors for each factor can be included in the packet drop estimation to eliminate the effect of such problem.

4.2. Wormhole Attack. One of the open research issues in the proposed schemes against wormhole attack is the consideration of the energy metric in the routing. As energy consumption is critical in WSNs, routing path which consumes less energy is important. Lack of the comprehensive attack detection methods is another open research issue. Although proposed detection methods use some features of wormhole attack to detect, detection methods which consider several features of the wormhole attack at the same time are not there. Since considering several features of the wormhole attack to detect attack can improve detection accuracy, it is important to consider several features at the same time while detecting. Moreover, more state-of-the-art research is required for this attack.

4.3. Sinkhole Attack. Similar to wormhole attack detection in sinkhole attack detection also comprehensive methods are needed. The proposed detection mechanisms mostly rely on the packet drop feature of the sinkhole attack to detect it. Spoofed, altered, or replayed routing information feature or some signs of the sinkhole attack are rarely considered in the detection. Moreover, detection methods based on the watchdog mechanism do not address problems related with watchdog mechanism, which we discuss above in the selective forwarding. More research is required in terms of quantity and quality in order to achieve state-of-the-art research in the field.

4.4. Sybil Attack. Research is done the least against this attack compared to other attacks in the research field. Research in terms of detection is in its initial stage. Proposed schemes which include a detection method consider irrelevant factors to detect such as packet drop and packet modification. Trust estimation methods are not addressed in many proposed schemes. Moreover, evaluation in terms of detection or

avoidance is rarely included in the proposed schemes. Most importantly we could not find any state-of-the-art research for this attack in the research field.

Open research issues in all proposed schemes and research field are as follows.

4.5. Trust Threshold. The research studies are needed, which tackle an optimal trust threshold under different scenarios, impact of trust threshold on the trust mechanism performance, and factors affecting trust threshold.

4.6. Accuracy of Estimated Trust Value. This issue also is not addressed in the proposed schemes. Proposed schemes simply assume that produced trust values are accurate and correct. Research study such as factors affecting accuracy of the trust value, considerations to achieve accurate trust value, and evaluation in terms of accuracy of estimated trust under different scenarios is needed.

4.7. Research on Other Routing Attacks. We could not find a considerable research work on HELLO flooding attack, acknowledgment spoofing attack, and spoofed, altered, or replayed routing information.

4.8. Comparison with Other Security Mechanisms. One of the open research issues is about merits and demerits of trust-based security compared to other security mechanisms to secure routing. As there are many other security mechanisms such as intrusion detection, insider attack detection mechanisms, and authentication-based mechanisms, it is important to demonstrate pros and cons of each security mechanism under different scenario.

4.9. Effect of Trust on Routing Performance. Routing performance can be affected by trust. For example, longer paths can be selected to avoid malicious nodes. Hence, research study which shows how negatively trust affects routing performance and how it can be minimized is important.

4.10. Multiple Attack Consideration. Proposed schemes are mostly designed for single attack. Trust establishment allows working based on the multiple attack detection. It might increase efficiency of trust establishment and improve security situation.

4.11. Design Factors and Considerations. Design factors and considerations of trust in routing can be guideline for researchers to design trust-based routing algorithm. Although research on design factors and considerations of trust for different fields is done, such research is lacking in applying trust in routing in WSNs.

5. Conclusions

In this research work, we attempted to demonstrate a research state of the trust-based routing from routing attack perspective. In order to give a better understanding of trust-based routing, first, overview of trust-based routing basics is discussed. Particularly we overview basics concepts of trust management, attack against routing protocol, and secure routing using trust mechanism. Then, proposed schemes are discussed and presented based on the attack which they are proposed against. To analyze proposed schemes efficiently and to provide more insight into them, we proposed dividing schemes into three components, which are learning, trust estimation, and routing. Hence, each proposed scheme is analyzed and discussed based on these three components. Moreover, we attempted to evaluate the proposed schemes based on the two important factors: energy consumption and attack resiliency/detection. After presenting proposed schemes, we discussed open research issues in the proposed schemes and research field in general, in which we pointed out several open research issues and recommendations to solve these issues.

Competing Interests

The authors declare no conflict of interests.

Acknowledgments

The present research has been conducted by the Research Grant of Kwangwoon University in 2017.

References

[1] F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, "Trust management system in wireless sensor networks: design considerations and research challenges," *Transactions on Emerging Telecommunications Technologies*, vol. 26, no. 2, pp. 107–130, 2015.

[2] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y.-J. Song, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 11, pp. 1698–1712, 2009.

[3] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: a survey," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 2, pp. 279–298, 2012.

[4] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," *Proceedings of the IEEE*, vol. 98, no. 10, pp. 1755–1772, 2010.

[5] H. Yu, Z. Shen, C. Miao, B. An, and C. Leung, "Filtering trust opinions through reinforcement learning," *Decision Support Systems*, vol. 66, pp. 102–113, 2014.

[6] H. Yu, Z. Shen, C. Leung, C. Miao, and V. R. Lesser, "A survey of multi-agent trust management systems," *IEEE Access*, vol. 1, no. 1, pp. 35–50, 2013.

[7] T. Qin, H. Yu, C. Leung, Z. Shen, and C. Miao, "Towards a trust aware cognitive radio architecture," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 13, no. 2, pp. 86–95, 2009.

[8] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, 2007.

[9] Y. Chae, L. C. Dipippo, and Y. L. Sun, "Predictability trust for wireless sensor networks to provide a defense against on/off attack," in *Proceedings of the 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom '12)*, Pittsburgh, Pa, USA, October 2012.

[10] C. J. Fung, J. Zhang, I. Aib, R. Boutaba, and R. Cohen, "Design of a simulation framework to evaluate trust models for collaborative intrusion detection," in *Proceedings of the International Conference on Network and Service Security (N2S '09)*, pp. 13–19, IFIP, Paris, France, June 2009.

[11] F. Ishmanov, S. W. Kim, and S. Y. Nam, "A robust trust establishment scheme for wireless sensor networks," *Sensors*, vol. 15, no. 3, pp. 7040–7061, 2015.

[12] Poonam, K. Garg, and M. Misra, "Trust based security in MANET routing protocols: a survey," in *Proceedings of the 1st Amrita ACM-W Celebration of Women in Computing in India (A2CWiC '10)*, Coimbatore, India, September 2010.

[13] G. Padmavathi and D. Shanmugapriya, "A survey of attacks security mechanisms and challenges in wireless sensor networks," *International Journal of Computer Science*, vol. 4, no. 1, pp. 1–9, 2009.

[14] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[15] H. Deng, X. Sun, B. Wang, and C. Yuanfu, "Selective forwarding attack detection using watermark in WSNs," in *Proceedings of the Second ISECS International Colloquium on Computing, Communication, Control, and Management (CCCM '09)*, pp. 109–113, August 2009.

[16] W. Cheng, X. Liao, C. Shen, S. Li, and S. Peng, "A trust-based routing framework in energy-constrained wireless sensor networks," in *Proceedings of the International Conference on Wireless Algorithms, Systems, and Applications (WASA '06)*, pp. 478–489, Xi'an, China, August 2006.

[17] Y. Cho and G. Qu, "Detection and prevention of selective forwarding-based denial-of-service attacks in WSNs," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 205920, 16 pages, 2013.

[18] L. C. DiPippo, Y. Sun, and K. Rahn, "Secure adaptive routing protocol for wireless sensor networks," Tech. Rep. TR10-329, 2010.

[19] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, "TSRF: a trust-aware secure routing framework in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 209436, 14 pages, 2014.

[20] F. Ghasemi, *Secure geographic routing in wireless sensor networks [Master of Science]*, University of Gothenburg, Gothenberg, Sweden, 2013.

[21] S. M. Sajjad, S. H. Bouk, and M. Yousaf, "Neighbor node trust based intrusion detection system for WSN," in *Proceedings of the 6th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN '15)*, pp. 183–188, Islamabad, Pakistan, September 2015.

[22] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Trust-based intrusion detection in wireless sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '11)*, June 2011.

[23] J. Ren, Y. Zhang, K. Zhang, and X. S. Shen, "Exploiting channel-aware reputation system against selective forwarding attacks in WSNs," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM '14)*, pp. 330–335, December 2014.

[24] K. Altisen, S. Devismes, R. Jamet, and P. Lafourcade, "SR3: secure resilient reputation-based routing," in *Proceedings of the 9th IEEE International Conference on Distributed Computing in Sensor Systems (DCoSS '13)*, Cambridge, Mass, USA, May 2013.

[25] Y. Hu, Y. Wu, and H. Wang, "Detection of insider selective forwarding attack based on monitor node and trust mechanism in WSN," *Wireless Sensor Network*, vol. 6, no. 11, pp. 237–248, 2014.

[26] O. Naderi, M. Shahedi, and S. M. Mazinani, "A trust based routing protocol for mitigation of sinkhole attacks in wireless sensor networks," *International Journal of Information and Education Technology*, vol. 5, no. 7, pp. 520–526, 2015.

[27] K. D. Kang, K. Liu, and N. Abu-Ghazaleh, "Securing geographic routing in wireless sensor networks," in *Proceedings of the 9th Annual Cyber Security Conference on Information Assurance*, pp. 38–39, Albany, NY, USA, June 2006.

[28] B. S. Kantariya and N. M. Shekokar, "Detection and mitigation of greyhole attack in wireless sensors network using trust mechanism," *International Journal of Science and Research*, vol. 4, no. 4, pp. 2500–2506, 2015.

[29] P. R. Vamsi and K. Kant, "An improved trusted greedy perimeter stateless routing for wireless sensor networks," *International Journal of Computer Network and Information Security*, vol. 6, no. 11, pp. 13–19, 2014.

[30] H. C. Leligou, P. Trakadas, S. Maniatis, P. Karkazis, and T. Zahariadis, "Combining trust with location information for routing in wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 12, no. 12, pp. 1091–1103, 2012.

[31] T. Zahariadis, P. Trakadas, S. Maniatis, P. Karkazis, H. C. Leligou, and S. Voliotis, "Efficient detection of routing attacks in wireless sensor networks," in *Proceedings of the 16th International Conference on Systems, Signals and Image Processing (IWSSIP '09)*, June 2009.

[32] Y. Liu, M. Dong, K. Ota, and A. Liu, "ActiveTrust: secure and trustable routing in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2013–2027, 2016.

[33] J. Kaur, S. S. Gill, and B. S. Dhaliwal, "Secure trust based key management routing framework for wireless sensor networks," *Journal of Engineering*, vol. 2016, Article ID 2089714, 9 pages, 2016.

[34] P. Gong, T. M. Chen, and Q. Xu, "ETARP: an energy efficient trust-aware routing protocol for wireless sensor networks," *Journal of Sensors*, vol. 2015, Article ID 469793, 10 pages, 2015.

[35] R. W. Anwar, M. Bakhtiari, A. Zainal, A. H. Abdullah, and K. N. Qureshi, "Enhanced trust aware routing against wormhole attacks in wireless sensor networks," in *Proceedings of the International Conference on Smart Sensors and Application (ICSSA '15)*, pp. 56–59, Kuala Lumpur, Malaysia, May 2015.

[36] J. Harbin, P. Mitchell, and D. Pearce, "Wireless sensor network wormhole avoidance using reputation-based routing," in *Proceedings of the 7th International Symposium on Wireless Communication Systems (ISWCS '10)*, pp. 521–525, IEEE, York, UK, September 2010.

[37] Z. Banković, D. Fraga, J. C. Vallejo, and J. M. Moya, "Improving reputation systems for wireless sensor networks using genetic algorithms," in *Proceedings of the 13th Annual Genetic and Evolutionary Computation Conference (GECCO '11)*, pp. 1643–1650, Dublin, Ireland, July 2011.

[38] J. M. Moya, J. C. Vallejo, D. Fraga, Á. Araujo, D. Villanueva, and J.-M. de Goyeneche, "Using reputation systems and non-deterministic routing to secure wireless sensor networks," *Sensors*, vol. 9, no. 5, pp. 3958–3980, 2009.

[39] S. Hazra and S. K. Setua, "Trusted routing in AODV protocol against wormhole attack," in *Future Information Technology, Application, and Service*, vol. 164 of *Lecture Notes in Electrical Engineering*, pp. 259–269, Springer, 2012.

[40] H. Liang, H. Fan, and F. Cai, "Defending against wormhole attack in OLSR," *Geo-Spatial Information Science*, vol. 9, no. 3, pp. 229–233, 2006.

[41] X.-F. Qiu, J.-W. Liu, and A. R. Sangi, "MTSR: wormhole attack resistant secure routing for Ad hoc network," in *Proceedings of the IEEE Youth Conference on Information, Computing and Telecommunications (YC-ICT '10)*, pp. 419–422, Beijing, China, November 2010.

[42] A. Pirzada, A. Datta, and C. McDonald, "Propagating trust in ad-hoc networks for reliable routing," in *Proceedings of the International Workshop on Wireless Ad-Hoc Networks*, Oulu, Finland, June 2004.

[43] T. H. Hai, E.-N. Huh, and M. Jo, "A lightweight intrusion detection framework for wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 10, no. 4, pp. 559–572, 2010.

[44] S. D. Roy, S. A. Singh, S. Choudhury, and N. C. Debnath, "Countering sinkhole and black hole attacks on sensor networks using dynamic trust management," in *Proceedings of the 13th IEEE Symposium on Computers and Communications (ISCC '08)*, pp. 537–542, IEEE, Marrakech, Morocco, July 2008.

[45] P. Samundiswary and P. Dananjayan, "Performance analysis of trust based AODV for wireless sensor networks," *International Journal of Computer Applications*, vol. 4, no. 12, pp. 6–13, 2010.

[46] P. Samundiswary and P. Dananjayan, "Secured dynamic source routing protocol for mobile sensor networks," in *Proceedings of the 12th International Conference on Networking, VLSI and Signal Processing*, pp. 19–23, Cambridge, UK, February 2010.

[47] P. Samundiswary, M. P. Kumar, and P. Dananjayan, "Trust based energy aware greedy perimeter stateless routing for wireless sensor networks," *Journal of Communication and Computer*, vol. 8, pp. 848–854, 2011.

[48] V. Salve and M. A. Bhalekar, "TARF-Trust Aware Routing Framework for wireless networks," *International Journal of Wireless Communications and Networking Technologies*, vol. 3, no. 4, pp. 73–77, 2014.

[49] P. R. Vamsi, P. K. Batra, and K. Kant, "BT-GPSR: an integrated trust model for secure geographic routing in Wireless Sensor Networks," in *Proceedings of the Students Conference on Engineering and Systems (SCES '14)*, Allahabad, India, May 2014.

[50] O. Powell, J.-M. Seigneur, and L. Moraru, "Trustworthily forwarding sensor networks information to the internet," in *Proceedings of the International Conference on Emerging Security Information, Systems, and Technologies (SECURWARE '07)*, pp. 30–35, Valencia, Spain, October 2007.

[51] A. Paul, S. Sinha, and S. Pal, "An efficient method to detect sybil attack using trust based model," in *Proceedings of the International Conference on Advances in Computer Science (AETACS '13)*, pp. 228–237, Elsevier, NCR, India, December 2013.

[52] V. Manjula and C. Chellappan, "Trust based node replication attack detection protocol for wireless sensor networks," *Journal of Computer Science*, vol. 8, no. 11, pp. 1880–1888, 2012.

[53] A. A. Atayero and S. A. Ilori, "Development of FIGA: a novel trust-based algorithm for securing autonomous interactions in WSN," in *Proceedings of the International Conference on Computer Science Applications (ICCSA '15)*, IAENG WCECS 2015, pp. 174–180, San Francisco, Calif, USA, October 2015.

[54] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: a trust-aware routing framework for WSNs," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 2, pp. 184–197, 2012.

[55] K. Gulaskar, A. Patel, R. Raut, and M. Japkar, "TBRF: trust based routing framework for WSNs," *International Journal of Electronics Communication and Computer Engineering*, vol. 5, no. 2, pp. 384–392, 2014.

[56] R. Amuthavalli and R. S. Bhuvaneswaran, "Genetic algorithm enabled prevention of sybil attacks for LEACH-E," *Modern Applied Science*, vol. 9, no. 9, pp. 41–49, 2015.

[57] P. Zhou, S. Jiang, A. Irissappane, J. Zhang, J. Zhou, and J. C. M. Teo, "Toward energy-efficient trust system through watchdog optimization for WSNs," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 613–625, 2015.

[58] A. D. Wood, L. Fang, J. A. Stankovic, and T. He, "SIGF: a family of configurable, secure routing protocols for wireless sensor networks," in *Proceedings of the 4th ACM Workshop on Security of ad hoc and Sensor Networks (SASN '06). A workshop held in conjuction with the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 35–48, Alexandria, Va, USA, October 2006.

[59] Z. Banković, D. Fraga, J. Moya et al., "Detecting and confining sybil attack in wireless sensor networks based on reputation systems coupled with self-organizing maps," in *Proceedings of the 6th IFIP Conference on Artificial Intelligence Applications & Innovations (AIAI '10)*, pp. 311–318, Larnaca, Cyprus, October 2010.

[60] D. B. Johnson, "Routing in ad hoc networks of mobile hosts," in *Proceedings of the Workshop on Mobile Computing Systems and Applications*, pp. 158–163, Santa Cruz, Calif, USA, December 1994.

[61] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF. RFC 3561, July 2003.

[62] P. Jacquet, P. Mühlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in *Proceedings of the 1st IEEE lnternational Multi Topic Conference (IEEE INMIC '01)*, pp. 62–68, IEEE, Lahore, Pakistan, December 2001.

[63] M. G. Zapata and N. Asokan, "Secure ad hoc on-demand distance vector routing," *ACM Mobile Computing and Communications Review*, vol. 3, no. 6, pp. 106–107, 2002.

[64] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Siences (HICSS '00)*, p. 223, Maui, Hawaii, USA, January 2000.