Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 232798, 10 pages
http://dx.doi.org/10.1155/2013/232798

Research Article

A Multipath Routing Approach for Secure and Reliable Data Delivery in Wireless Sensor Networks

Hind Alwan and Anjali Agarwal

Department of Electrical and Computer Engineering, Concordia University, Montreal, QC, Canada H3G 1M8

Correspondence should be addressed to Hind Alwan; h_alwan@encs.concordia.ca

Received 28 September 2012; Revised 22 December 2012; Accepted 30 January 2013

Academic Editor: Marc St-Hilaire

Copyright © 2013 H. Alwan and A. Agarwal. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The severe resource constraints and challenging deployment environments of wireless sensor networks (WSNs) pose challenges for the security and reliability of data transmission for these networks. In this paper, we present and evaluate a secure and reliable routing mechanism offering different levels of security in an energy-efficient way for WSNs. Our approach uses node-disjoint routing and the selection mechanism of these paths depends on different application requirements in terms of security. The original data message is split into packets that are coded using Reed-Solomon (RS) codes and, to provide diverse levels of security, different number of fragments is encrypted related to the requested security level before being transmitted along independent node-disjoint paths. This technique makes encryption feasible for energy-constrained and delay-sensitive applications while still maintaining a robust security protection. We describe how to find the secure multipath, the number of these paths, and how to allocate fragments on each path seeking to enhance security and improve data reliability. Extensive analysis and performance evaluation show that data transmission security and reliability can be enhanced while respecting the resource constraints of WSNs.

1. Introduction

Advances in wireless sensor networks have enabled a wide range of application across many fields. Many of these applications have high quality of service (QoS) requirements in terms of security and reliability of data transmission.

Wireless sensor networks (WSNs) are characterized by severe resource constraints of sensor nodes, unreliable nature of the wireless links, dynamic changing in the size and density of the network, and the high risk of physical attacks to sensors. Many routing protocols have been proposed to overcome these constraints and improve the QoS in wireless networks. However, most of the existing protocols provide either secure [1] or QoS [2–5] routing. Few protocols have combined these two requirements [6–9].

Secure multipath routing protocols in WSNs can be divided into three categories based on the security-related operational objective [1]. The multipath routing protection only, the attack-specific, and the security operations support. The security-based multipath routing protection protocol is the interest of this paper in which the multipath routing is used to improve the security, increase reliability of data transmission, provide load balancing, and decrease the end-to-end delay.

A common approach to provide reliability in WSNs is to use forward error correction (FEC) technique as a replication mechanism in multipath routing to increase data transmission reliability, decrease energy consumption, and increase the network lifetime while avoiding the costly or impossible data retransmission due to the severe resource constraints of sensor nodes [10]. However, this approach required sending more data than necessary over the multipath in order to tolerate a certain number of path failures.

This paper was motivated mainly by the observations that most traditional encryption algorithms are complex and may introduce a severe delay in sensor nodes. For instance, the encryption time of each 128-bit block using the AES algorithm is about 1.8 ms on a MicaZ platform [11]. Our approach therefore proposes to encrypt only a certain fraction of the RS [12] codewords while the remaining portion is transmitted unprotected. Our scheme makes encryption feasible for energy-constrained and delay-sensitive applications while still maintaining a robust security protection.

Our major contributions in this paper are the following. First, we introduce a new mechanism for secure and reliable data transmission in WSNs multipath routing, derived from node-disjoint multipath and combined with source coding in order to enhance both security and reliability of data transmission in the network. Second, we define different levels of security requirements and depending on these requirements, a selective encryption scheme is introduced to encrypt selected number of coded fragments in order to enhance security and thereby reduce the time required for encryption. Finally, an allocation strategy that allocates fragments on paths is introduced to enhance both the security and probability of successful data delivery.

The remainder of this paper is organized as follows. In the next section, we review the related work on secure and reliable multipath routing protocols. The routing problem metrics are formulated in Section 3. Section 4 provides a detailed description of the proposed secure mechanism. In Section 5, we describe our methodology for evaluating the security and reliability. A detailed case study is presented with different required security levels and possible attack scenarios. The simulation model and the performance evaluation are presented. Finally, we conclude our work in Section 6.

2. Related Work

In the literature, encryption techniques have been developed for secure multipath routing protocols in WSNs. In [1], an extensive survey has been conducted on the current state of the art for secure multipath routing protocols. The security-related issues, threats, and attacks in WSNs and some of the solutions can be found in [13].

One of the possible solutions to support secure and reliable data transmission is to combine multipath routing protocols with secret sharing algorithm. In (T, N) threshold secret sharing algorithm [14], the original data message is divided into N shares and sent to the destination over different paths. The original message can be reconstructed from any T shares, while no information about the original message can be obtained with less than T shares. The main drawback of using the secret sharing method is the large amount of traffic and redundancy involved. H-SPREAD [6] protocol is proposed as an extended version of SPREAD protocol [7] which used multipath between a single source-destination pair to deliver multiple secret message shares in order to enhance the data confidentiality in mobile ad hoc networks. H-SPREAD proposed for WSNs a distributed many-to-one multipath discovery protocol by employing two phases of flooding in order to enhance the security and reliability of data transmission. To enhance reliability, H-SPREAD uses an active per-hop packet salvaging strategy; the sender forwards the packet over another path instead of dropping it when unsuccessful transmission occurs to increase the probability that the data packet is delivered to the sink. Although, H-SPREAD protocol provides security in terms of resilience against node capture, it does not provide any authentication mechanism. Thus, many network layer attacks such as Sinkhole or Wormhole on routing protocols that attract traffic by advertising high-quality route to the sink are related with the goal of affecting the construction of paths. Furthermore, the construction of the spanning tree used in this protocol introduces high overhead.

Other possible solutions to support secure and reliable data transmission is the combination of data encryption and FEC technique [8, 9]. The main concept of this combination is to encrypt the original data message, encode the encrypted message using FEC coding, and then route it to the destination. A secure, multiversion, multipath protocol, MVMP, is proposed in [9] to offer a secure and reliable data communication in WSNs. MVMP consists of four steps: divide the original data message into groups, encrypt each group using different cryptographic algorithms, code the encrypted packets using RS codes, and transmit the coded packets on multiple disjoint paths that are assumed to be established before the data transmission. The data packet can be compromised when certain amount of codewords over different paths are intercepted and all the encryption algorithms used for the transmission are known. Moreover, to reconstruct the original message, the attacker needs to make all possible packet combinations, which is a resource challenging task. Although MVMP protocol uses different cryptographic algorithms in order to enhance data transmission security; this strategy could be expensive in resource-constrained environments such as WSN.

In [15], a secure and reliable node-disjoint multipath routing protocol is proposed in order to minimize the worst case security risk and to maximize the packet delivery ratio under attacks. The multipath routing problem is modeled as an optimization problem and solved by a heuristic algorithm using game theory, and a routing solution is derived to achieve a tradeoff between route security and delivery ratio in worst scenarios. The protocol focuses on the worst case attack scenarios to achieve the design objective of providing the best security and/or delivery ratio. Although the protocol assumes using link reliability history in the computations, in WSN the sensors and the communication links change frequently and are time varying. This required a frequent update of the computation of paths to discover the most reliable and secure paths. Also, the protocol assumes that each node has a full knowledge of the whole network topology which is considered an expensive assumption in WSN.

An intrusion-fault tolerant routing scheme proposed in [16] offers a high level of reliability by a secure multipath routing construction topology and uses one-way hash chains to secure the construction of a multipath, many-to-one dissemination topology.

A secure and energy-efficient multipath routing protocol for wireless sensor networks is proposed in [17]. Disjoint and braided paths are constructed using a modification of the breadth first search algorithm. The sink executes the paths discovery, selection, and maintenance in a centralized way. The authors claim that network layer attacks such as Sinkhole and Wormhole are not related since routing paths are selected by the sink node and periodically changed to prolong the lifetime of the network. Also, the protocol addresses the replayed attack by having each packet identified by a unique sequence number to be transmitted only once. However, the protocol does not use any encryption and authentication mechanism to protect against a number of attacks; this means

that an attacker can affect the paths construction process. Moreover, the sink needs to have information of the whole network topology which requires that each node sends its neighbors list to the sink, and this process consumes huge energy and introduces extra overhead.

Enhancing data security in ad hoc networks based on multipath routing is proposed in [18], which is designed on the multipath routing characteristics of ad hoc networks and uses a route selection based on the security costs without modifying the lower layer protocols. The authors claim that the proposed protocol can be combined with solutions which consider security aspects other than confidentiality to improve significantly the efficiency of security systems in ad hoc networks. The protocol in [18] is designed for an ad hoc network where the number of nodes in the network is considerably low and the capability of node is usually better than that of sensor networks. Thus, the protocol cannot directly fit the properties of sensor networks.

Our work differs from the above existing schemes by considering different levels of security requirements to encrypt limited number of packets contingent to these requirements in order to enhance data transmission security at lower cost than full packet encryption. The new mechanism proposed adapts to the resource constraints of WSNs by combining FEC technique and selective cryptographic algorithms to achieve secure and reliable data transmission in an energy-efficient way for WSNs. Unlike [9], the original message is split into packets that are first coded using RS codes. Then depending on the required security level, the selective encryption scheme is used to encrypt a selected number of coded fragments before being transmitted along different disjoint paths. Thus, the security can be achieved while respecting the resource constraints of WSNs.

3. QoS Routing Problem Formulation

3.1. Replication and Erasure Coding. Erasure coding has been used in distributed systems to achieve load balancing and fault tolerance, but recently [10] it has been used for WSNs as a replication mechanism in multipath routing to increase the data transmission reliability while decreasing energy consumption and increasing network lifetime. The advantage of using data replication is to avoid the costly or impossible data retransmission in WSNs due to the severe resource constraints of sensor nodes. RS code is the simplest and the widely used FEC codes for achieving reliable data transmission in networks.

In the network layer, we assume that there are totally n available disjoint paths between the source node and the sink. Only the source node and the sink are active participants in the coding/decoding process while no processing is needed at the intermediate nodes. Using RS codes, the source node codes each data packet of size Mb bits it receives into M fragments each of size b bits and generates another K parity fragments to have in total a set of $M + K$ fragments. If the sink receives any M fragments, it can recover the original data packet allowing at most K lost fragments. Denote the fragments allocation as $X = [x_1, x_2, \ldots, x_n]$, where x_i is an integer and is the number of fragments allocated to path_i and n is the number of node-disjoint paths from source node to sink, as shown in Figure 1 [10]. The allocation of fragments on each path is determined with a load balancing algorithm where $\sum_{i=1}^{n} x_i = M + K$. The value of K determines the loss recovery capability of the code. Given a fixed value of $M + K$, smaller M means less data information and more redundancy contained in each encoded block, thus the loss, recovery capability is better. If z_i is a random variable that indicates the number of fragments received on path_i, then we have $\sum_{i=1}^{n} z_i \geq M$. Typically, the code rate is $\lambda = M/(M+K)$, the redundancy ratio is $r = K/(M + K)$, the maximum codeword length for a RS code is $c = 2^b - 1$, and the coding overhead is $h = K/M$.

3.2. Security. A path is compromised when one or more node in the path is compromised. In this paper, node-disjoint paths are used; vthus the probability of compromising of a single path is not correlated with the probability of compromising of other paths. We assume that the source node and the sink are trustworthy. The source node selects np paths out of the n node-disjoint paths to route the data packet to the sink. The probability that the data packet is compromised, P_{pkt}, is defined as

$$P_{\text{pkt}} = \prod_{i=1}^{np} P_{\text{path}_i}, \tag{1}$$

where P_{path_i} is the probability that path_i is compromised and is given as

$$P_{\text{path}_i} = 1 - \prod_{u=1}^{l} (1 - p_u), \tag{2}$$

where p_u is the probability that a sensor node is compromised, $u \in l$, l is the number of sensor nodes on path_i and $0 \leq P_{\text{path}_i} \leq 1$.

Note that the probability p_u indicates the security level of node u and could be estimated from the feedback of some security-monitoring software or hardware such as firewalls and intrusion detection devices [18].

The proposed mechanism uses RS coding to send the $M + K$ fragments on np node-disjoint paths. To improve the security of the data transmission consider the following.

(1) Allocate fragments on as many paths as possible in order to minimize the probability P_{pkt}. The total number of fragments for each packet is equal to np, that is $M + K = np$. In this case, one fragment is transmitted on each path. With such allocation, the probability that the data packet is compromised, P_{pkt}, is equal to the probability that M out of np paths are compromised, $P_{\text{pkt}} = \prod_{i=1}^{M} P_{\text{path}_i}$. Thus, the more paths are used, the less P_{pkt} is, and the better the security is, Figure 2.

However, this strategy could be expensive in resources constraint networks like WSNs since it introduces a large storage and communication overhead. Moreover, fragments might be dropped on some paths due to the error-prone nature of sensor nodes and wireless links and to reconstruct the original data packet, a minimum of M paths are needed

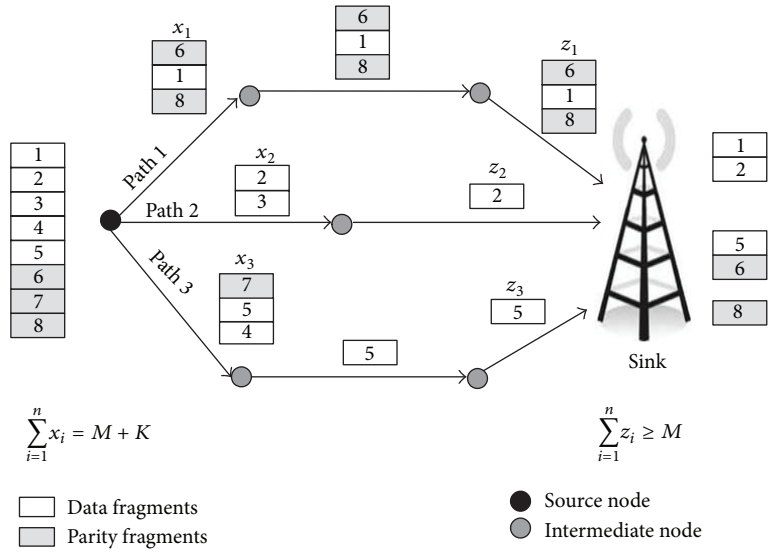


FIGURE 1: Example of data transmission using erasure coding [10]. Note that the data packet $M = 5$ fragments, the added redundancy $K = 3$ fragments and $n = 3$ paths.

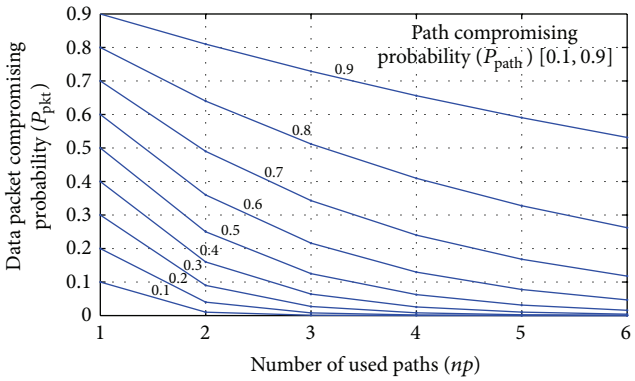


FIGURE 2: Relationship between data packet compromising probability, P_{pkt}, and the number of used paths, np, for different path compromising values, $P_{path_i}[0.1, 0.9]$.

to successfully deliver the required number of fragments to the sink.

(2) To achieve the highest security level, the allocated fragments on any path, x_i, should be less than M. With such allocation an attacker must intercept more than one path to get the M fragments required to reconstruct the data packet. The allocated fragments on each path should be as follows:

$$1 \leq x_i \leq M - 1. \tag{3}$$

This strategy is used in the proposed security mechanism.

(3) Minimize P_{path_i} such that P_{pkt} is minimized, (1). By using a path that contains as few nodes as possible, the shortest path and/or, path that contains the highest secure nodes among others minimizes P_{path_i}, (2).

3.3. Reliability. Multipath routing is one way of improving the reliability of data transmission by sending duplicated data via multiple paths. Thus, a packet is delivered to the destination even if some paths fail. The main drawbacks of the multipath routing are the higher energy consumption and the high probability of network congestion due to the increased number of messages which in turn impact the performance of the network. However, to improve the reliability of data transmission while respecting the network energy constraint, redundancy is applied using erasure coding on multipath routing. The idea is to send more fragments, $M + K$, than the minimum required fragments, M, to recover the original packet at the sink. In our proposed routing mechanism, the reliability of data transmission, the successful end-to-end data delivery, is achieved by sending the fragments of RS codeword on np selected node-disjoint multipath and to guarantee that the codeword packet is recoverable from any $\lceil np/2 \rceil$ paths, we need to ensure that fragments allocation on any $\lceil np/2 \rceil$ paths follows,

$$\sum_{i=1}^{\lceil np/2 \rceil} x_i \geq M. \tag{4}$$

3.4. Delay. The total path delay, D_{path}, includes the sum of time required for processing, queuing, transmission and propagation for all the nodes along the path. If coding and encryption are used, the path delay equals ($D_{path} + D_{cod} + D_{enc}$), where D_{cod} and D_{enc} are the coding time and the encryption time, respectively. D_{enc} is related to number of bits to be encrypted, n_{bit}, the unit-block encryption time, T_{blk}, and the encryption block size, L_{blk}, [19]. This is given as follows,

$$D_{enc} = \left(\frac{n_{bit}}{L_{blk}} \right) T_{blk}. \tag{5}$$

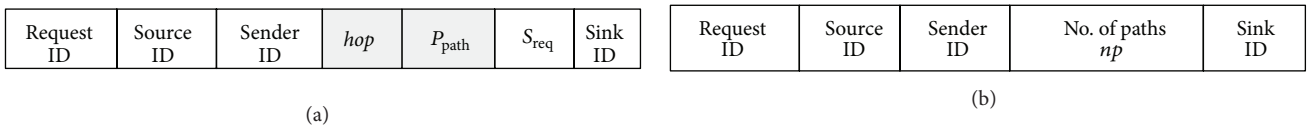


Figure 3: Control messages format (a) route request message, *RREQ*, (b) route reply message, *RREP*.

Encryption block size varies between different encryption algorithms and may also vary within the same encryption algorithm while the unit-block encryption time can be measured on specific platforms. Thus, choosing the appropriate block size as well as the total amount of bits to be encrypted can affect the delay performance of the network. Therefore, in our proposed selective encryption approach, a minimum amount of data is selected for encryption contingent to the security requirements. In this way, encryption time is reduced due to the need to encrypt fewer packets. Also, the energy required to encrypt the extra packets is conserved while still maintaining the required security level.

4. Proposed Protocol

An on demand routing protocol [20] is used to build multiple disjoint paths using route request/reply phases. Each sensor node is assumed to update the local states of its one-hop neighbors by broadcasting a *HELLO* message in which the links conditions are reported. Each node then maintains and updates its neighboring table information to record the link performance between itself and its direct neighbor nodes in terms of the probability that a sensor node is compromised, p_u. When the source node has data packet to transmit to the sink to which it has no available route, it starts the route discovery phase by transmitting a short route request message, *RREQ,* as shown in Figure 3(a). An *RREQ* message is broadcasted to all the neighbors of the source node within its transmission range, in which the required security level (in terms of message compromising probability), S_{req}, the path information (hop, P_{path}) are transferred to the sink. Each intermediate node updates the information of its one-hop local states, including the path compromising probability and hop count information. The route discovery phase is therefore introduced.

4.1. Next Node Selection. In order to achieve the shortest hop count from the current node to the sink, we assume that only the neighbors that are closer to the sink than the current node are added to the neighbor list as a candidate node. Since security is the essential metric in choosing different paths and to maximize the path security (Section 3), and to ensure constructing node-disjoint paths, each intermediate node selects one node as the next hop from its neighbor list to forward the *RREQ*, the neighbor with the highest security among all, smallest p_u. However, if the selected node is already reserved then the next neighbor with the smallest p_u will be selected and so on. The selected node then modifies the path information in the *RREQ* message (hop and P_{path_i} in Figure 3(a)), before forwarding the message to the next selected neighbor. The probability of path compromising, P_{path}, is updated according to (2) and the value of hop count, hop, is increased by one. Note that the initial values of hop and P_{path_i} at the source node are zero.

4.2. Number of Path Selection. The sink estimates the number of all available node-disjoint paths to the source from the number of the *RREQ* messages received to decide on choosing the first np most secure paths that satisfy the required security level. From these *RREQ* messages it obtains information about security and number of hops on each path. The sink sends back the route reply message, *RREP*, Figure 3(b), via the selected paths. Algorithm 1 is used to determine the number of node-disjoint multipath, np, which are used to transmit data message between the source and the sink. For each data transmission, given n available node-disjoint paths between the source and the sink, the sink sorts these available paths according to the security characteristics of each path (in terms of the probability that path i is compromised), such that the first path is the highest secure one and so on. The sink then calculates the probability that a packet is compromised, P_{pkt}, using (1). According to (1) more paths are chosen to lower P_{pkt} and enhance the security in order to deliver the data packet. Our proposed protocol only needs to select the first np paths ($np \geq 2$) satisfying $P_{pkt} \leq (1 - S_{req})$.

4.3. Security Mechanism. The following consecutive steps are involved in the routing mechanism to ensure the communication security level and are illustrated in Figure 4 [21].

(1) Divide the original data message of size S into j packets each of M fragments of size b bits. Assume the number of packets is equivalent to the number of paths used to transmit the data, np, such that $Mb = \lceil S/np \rceil$. If the last packet is less than M fragments, zero padding [9] is applied to meet the length requirements of RS codes.

(2) Encode each packet using RS codes to generate M data fragments and K parity fragments as a codeword of size $M+K$ fragments such that $K \leq M$. For each codeword packet, allocate one fragment on each path starting from the highest secure path and repeat this process till all the $M+K$ fragments are assigned on the selected multipath and ensure that the number of allocated fragments on each path, x_i, follows

$$x_i = \left\lceil \frac{(M+K)}{np} \right\rceil < M, \quad i = 1, 2, \ldots, np. \tag{6}$$

(3) Depending on the required security level, the number of fragments to be encrypted, N_{enc}, is calculated as follows:

$$N_{enc} = K + E, \tag{7}$$

where E is determined according to the required security level and $1 \leq E \leq M$.

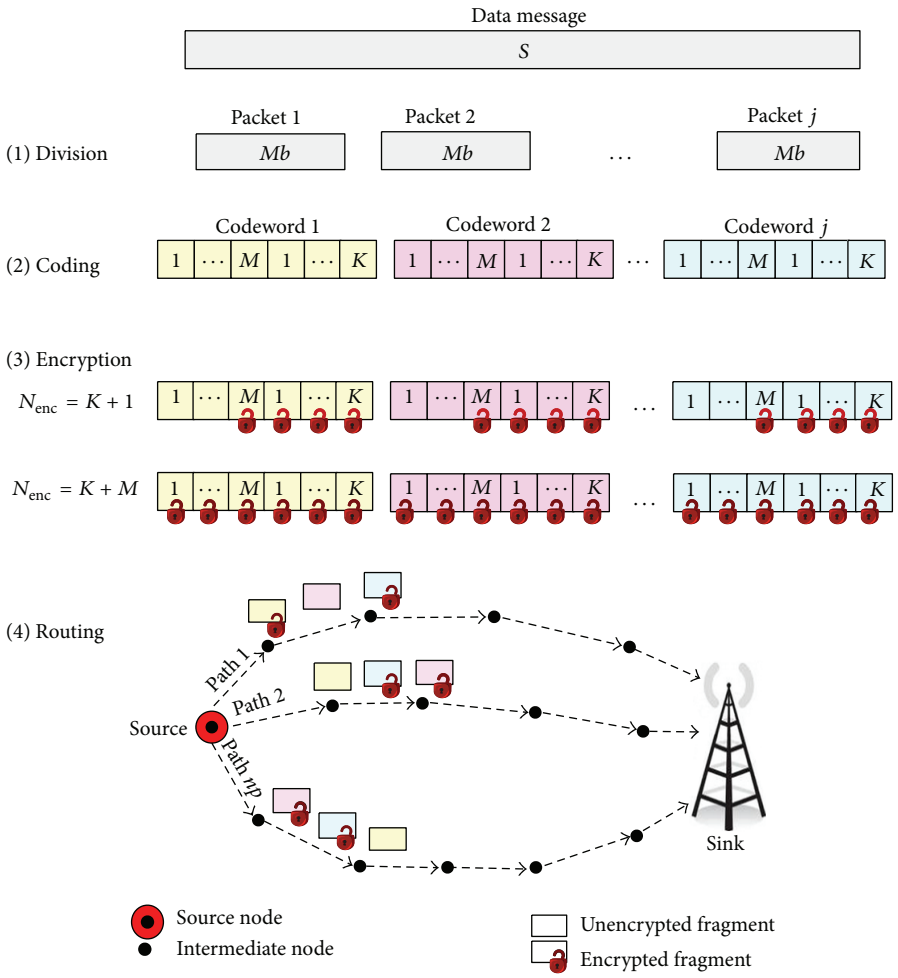


Figure 4: Proposed security mechanism.

As shown in Figure 4, for a low security requirement, $E = 1$, source node only encrypts any $N_{enc} = K + 1$ of $M + K$ fragments from the codeword. For each codeword, an attacker must receive at least M of the $M + K$ fragments and be able to decrypt the encrypted fragments to restore the codeword. On the other hand, when the required security level is high, then $E = M$, which requires to encrypt $N_{enc} = K + M$ fragments for each codeword. In order to compromise the data packet, the attacker must receive and be able to decrypt all M fragments to reconstruct the codeword.

(4) Route all the fragments on the np node-disjoint paths to the sink with each path carrying x_i fragments according to (4) and (6). To enhance security the encrypted fragments from the same codeword are transmitted on different paths.

(5) At the sink side, the encrypted fragments are decrypted first and then all the fragments are decoded to reconstruct the original data packet.

5. Evaluation Methodology

In this section, we precisely explain the security and reliability behaviors of the proposed mechanism. For security metric, we describe different scenarios to compromise the data packet, and for the reliability metric, we describe the failure models for which we evaluate the resiliency of our mechanisms.

5.1. Case Study. To help illustrate, we present an example on how the proposed mechanism functions with diverse security levels and attacker scenarios. Suppose we have a 9-byte data message to be transmitted to the sink. Let $np = 3$ and assume using packet-level RS (5, 3) code, where $M = 3$ and $M+K = 5$. Bit-level RS can also be used. The RS codeword packet has the following matrix format:

$$\text{RS codeword} = \begin{pmatrix} d_{j,1} \\ \vdots \\ d_{j,M} \\ p_{j,1} \\ \vdots \\ p_{j,K} \end{pmatrix}, \tag{8}$$

where $d_{j,1} \cdots d_{j,M}$ and $p_{j,1} \cdots p_{j,K}$ are the data and parity fragments for codeword j, respectively.

```
n = number of available node-disjoint paths (source to sink)
Sort for P_path such that P_path_1 < P_path_2 < ··· < P_path_n
np = 1;                          //Initialization
P_pkt_1 = P_path_1               //Calculate the probability of compromising a packet on the first path
for (i = 2; i ≤ n; i++)
{
np = np++;
P_pkt_i = P_pkt_i−1 × P_path_i
If (P_pkt_i ≤ (1 − S_req))       //if the required security is reached
   {
      number of paths to be used = np;
      break;
   }
}
```

Algorithm 1: Calculating the number of paths related to the required security level.

Step 1 (*division*). For $np = 3$, divide the 9 byte data message to three packets of the size of 3-byte.
Step 2 (*coding*). The three packets are coded using RS code to generate three codewords each of the size of 5-byte as follows:

$$\text{Codeword 1} = \begin{pmatrix} d_{1,1} \\ d_{1,2} \\ d_{1,3} \\ p_{1,1} \\ p_{1,2} \end{pmatrix},$$

$$\text{Codeword 2} = \begin{pmatrix} d_{2,1} \\ d_{2,2} \\ d_{2,3} \\ p_{2,1} \\ p_{2,2} \end{pmatrix}, \tag{9}$$

$$\text{Codeword 3} = \begin{pmatrix} d_{3,1} \\ d_{3,2} \\ d_{3,3} \\ p_{3,1} \\ p_{3,2} \end{pmatrix}.$$

Step 3 and 4 (*encryption and routing*). Depending on the required security level, encrypt any N_{enc} fragments, (7), for each codeword using any encryption algorithm and allocate fragments on np paths according to (4) and (6).

Scenario 1. For low security requirement, $N_{\text{enc}} = K + 1$, $N_{\text{enc}} = 3$ fragments:

$$\begin{pmatrix} d_{1,1} \\ d_{1,2} \\ d_{1,3} \\ p_{1,1} \\ p_{1,2} \end{pmatrix} \begin{pmatrix} d_{2,1} \\ d_{2,2} \\ d_{2,3} \\ p_{2,1} \\ p_{2,2} \end{pmatrix} \begin{pmatrix} d_{3,1} \\ d_{3,2} \\ d_{3,3} \\ p_{3,1} \\ p_{3,2} \end{pmatrix} \tag{10}$$

$$\text{path}_1 = d_{1,1}, p_{1,1}, d_{2,2}, p_{2,2}, d_{3,3}$$

$$\text{path}_2 = d_{1,2}, p_{1,2}, d_{2,3}, d_{3,1}, p_{3,1}$$

$$\text{path}_3 = d_{1,3}, d_{2,1}, p_{2,1}, d_{3,2}, p_{3,2}.$$

In this scenario, the attacker must intercept at least two paths and decrypt six fragments to get the three codewords.

Scenario 2. For moderate security requirement, $N_{\text{enc}} = K+2$, $N_{\text{enc}} = 4$ fragments.

$$\begin{pmatrix} d_{1,1} \\ d_{1,2} \\ d_{1,3} \\ p_{1,1} \\ p_{1,2} \end{pmatrix} \begin{pmatrix} d_{2,1} \\ d_{2,2} \\ d_{2,3} \\ p_{2,1} \\ p_{2,2} \end{pmatrix} \begin{pmatrix} d_{3,1} \\ d_{3,2} \\ d_{3,3} \\ p_{3,1} \\ p_{3,2} \end{pmatrix} \tag{11}$$

$$\text{path}_1 = d_{1,1}, p_{1,1}, d_{2,2}, p_{2,2}, d_{3,3}$$

$$\text{path}_2 = d_{1,2}, p_{1,2}, d_{2,3}, d_{3,1}, p_{3,1}$$

$$\text{path}_3 = d_{1,3}, d_{2,1}, p_{2,1}, d_{3,2}, p_{3,2}.$$

The attacker must intercept at least two paths and decrypt eight fragments to get the three codewords.

Scenario 3. For high security requirement, $N_{\text{enc}} = K + M$, $N_{\text{enc}} = 5$ fragments:

$$\begin{pmatrix} d_{1,1} \\ d_{1,2} \\ d_{1,3} \\ p_{1,1} \\ p_{1,2} \end{pmatrix} \begin{pmatrix} d_{2,1} \\ d_{2,2} \\ d_{2,3} \\ p_{2,1} \\ p_{2,2} \end{pmatrix} \begin{pmatrix} d_{3,1} \\ d_{3,2} \\ d_{3,3} \\ p_{3,1} \\ p_{3,2} \end{pmatrix} \tag{12}$$

$$\text{path}_1 = d_{1,1}, p_{1,1}, d_{2,2}, p_{2,2}, d_{3,3}$$

$$\text{path}_2 = d_{1,2}, p_{1,2}, d_{2,3}, d_{3,1}, p_{3,1}$$

$$\text{path}_3 = d_{1,3}, d_{2,1}, p_{2,1}, d_{3,2}, p_{3,2}.$$

In this scenario, the attacker needs to intercept at least two paths and be able to encrypt a total of ten fragments to get the three codewords.

For all the above scenarios, an attacker needs to decode each codeword to be able to reconstruct the original data message and the allocation of fragments on the paths, allowing for

Table 1: Multipath routing protocols comparison.

Protocol	No. of transmitted packets	No. of redundant packets	No. of encrypted packets	Redundancy ratio
MVMP [9]	$\lceil S/M \rceil \times (M+K) = 15$	$\lceil S/M \rceil \times K = 6$	$\lceil S/M \rceil \times M + K = 15$	$K/(M+K) = 40\%$
Threshold secret sharing scheme	$S \times N = 27$	$(N-1) \times S = 18$	$S \times N = 27$	$(N-1)/N = 66.6\%$
Proposed scheme	$\lceil S/np \rceil \times (M+K) = 15$	$np \times K = 6$	$K + E = [3, 15]$	$K/(M+K) = 40\%$

Table 2: Simulation parameters.

Parameters	Value
Scenario 1	100% of nodes, $p_u = 0.14$
Scenario 2	10% of nodes, $p_u = 0.50$ 40% of nodes, $p_u = 0.20$ 50% of nodes, $p_u = 0.02$
S_{req}	$(1-10^{-1})$ to $(1-10^{-10})$ Lowest to highest

resilience to a failure of one path, which can be any path, since the three data fragments for each codeword can be obtained from the other two paths.

5.2. Multipath Protocol Performance Evaluation. In this section, we evaluate the proposed mechanism using the same scenario presented in Section 5.1 and compare it with the protocols that used the (T, N) threshold secret sharing scheme [6, 7] and RS coding technique, MVMP [9]. We present the comparison in Table 1 in terms of the total number of transmitted, redundant, and encrypted packets as well as the coding redundancy ratio.

Clearly, the number of encrypted packets in MVMP protocol is equal to the encrypted packet of our proposed protocol when the demanded security level is high. However, when the demanded security level is low, our proposed protocol encrypts only three packets while MVMP protocol has a fixed number of fifteen encrypted packets. Note that encrypted packets influence encryption time and energy consumption. We recognize that the encryption delay is related to the total amount of bits to be encrypted for each data packet (Section 3.4). Thus, the proposed security mechanism selects a minimum amount of data for encryption. In WSNs, if sensors run different encryption algorithms, like in MVMP protocol, it may lead to varying computational delays. For instance, the traditional RC4 algorithm takes 344 μsec to encrypt a block on the Atmega103 processor; however, it only takes 10 μSec on the StrongARM processor [22]. Also in [23], the experiment results show that the encryption process of RC5 algorithm consumes more energy than that of AES on MicaZ platform. Moreover, our proposed security mechanism uses one encryption algorithm while still maintaining a robust security protection unlike MVMP protocol where multiple versions of encryption algorithms are used to maintain the security.

We have conducted an extensive simulation study using C++ to evaluate the performance of our protocol. We adapted the same codes used in our previously published works [20, 24]. These papers illustrated the validity and comparability of our implementation, in which the validation tests cover

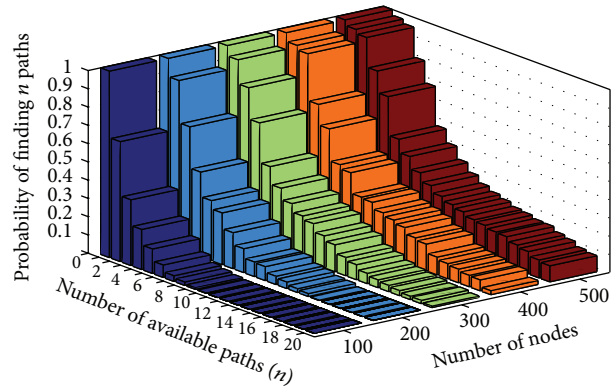


Figure 5: Probability of finding n node-disjoint paths.

the basic functionality of the on-demand routing protocol in WSNs. In WSNs, the likelihood of finding node-disjoint paths increases at higher node densities [25]. Thus, in order to increase the probability of finding these paths to evaluate the performance of our proposed protocol, we consider a network where 100 to 500 nodes are randomly scattered in a field of 500 m × 500 m area. We assume that all sensor nodes are static after deployment with transmission range of 100 m. The simulation parameters that we use are as follows. Source nodes are picked randomly, at least two hops away from the sink, to transmit a data packet at fixed generation rate of 1 packet/sec. The simulation time is 750 sec.

We use two types of security scenarios in each simulation. In Scenario 1, each node is assumed equally likely to be compromised with probability, $p_u = 0.14$. In the second scenario and to evaluate the worst case where the probability that a sensor node is compromised, p_u, is changed suddenly at any transmission instant and is randomly distributed as presented in Table 2. Simulation results are obtained from different configurations to reduce the effect of the position of sensors. The results shown are averaged over 10 simulation runs.

The proposed mechanism depends on the availability of finding multiple node-disjoint paths and to justify the possibility of finding these paths in WSNs, the security requirements are not considered in this step. Figure 5 shows the probability of finding the maximal number of node-disjoint paths between the source nodes and the sink. As the number of paths found in both scenarios is equal, we only report one result in Figure 5, and this indicates that the process of finding the maximum number of paths depends on the network topology only.

Figures 6 and 7 illustrate the security performance and the number of used paths for various network sizes (500 and

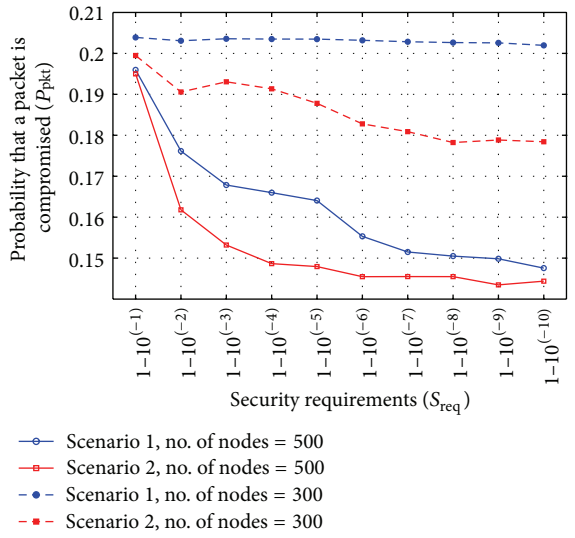


FIGURE 6: Security requirements (S_{req}) versus packet compromise probability (P_{pkt}),

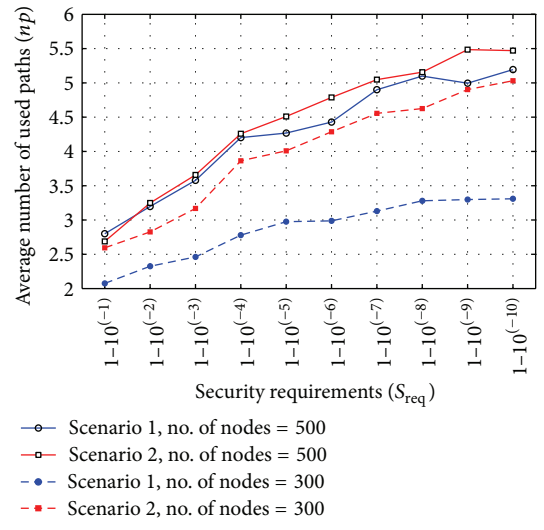


FIGURE 7: Security requirements (S_{req}) versus average number of used paths (np).

300 nodes) as a function of the requested security. A message is compromised when at least M fragments are received and N_{enc} fragments are decrypted. It means $\lceil np/2 \rceil$ paths are intercepted out of the np used paths. It is clear that our mechanism is effective in increasing the security performance of a message according to the requested security. The probability that the message is compromised decreases with the increase of the security requirements since the number of paths used is related to these requirements. This result verifies the effectiveness of our mechanism. We also observe that when nodes are with different security levels (Scenario 2), our algorithm tends to select more secure paths compared to Scenario 1. However, in both scenarios, the probability that the message is compromised increases as the number of nodes increases. When the number of nodes increases, there are more sensor nodes available for forwarding packets.

In Figure 8, the number of encrypted fragments (N_{enc}) for different values of parity fragments ($K = 1, 2, \ldots, K \leq M$) are presented. The data packet is set to $M = 10$ fragments. The number of encrypted fragments used in MVMP mechanism is compared with the lowest and the highest security requirements in our proposed protocol. The other S_{req} values show the same trend (between the two curves) and therefore are omitted. In MVMP mechanism all the fragments of the coded packet ($M + K$) are encrypted. Thus, the number of encrypted fragments using MVMP mechanism equals the number of encrypted fragments of the proposed mechanism at the highest security requirements. Clearly, the number of encrypted fragments is higher for the highest security requirement ($S_{req} = 1–10^{-10}$) to the encrypted fragments of the lowest security requirement ($S_{req} = 1–10^{-1}$); from 81.82% to 45% less fragments are encrypted for the lowest security requirement for $K = 1$ to 10, respectively. Obviously, when the demanded security level is high, our proposed protocol encrypts $K + M$ fragments similar to MVMP mechanism. However, when the demanded security level is low, $M + 1$ are

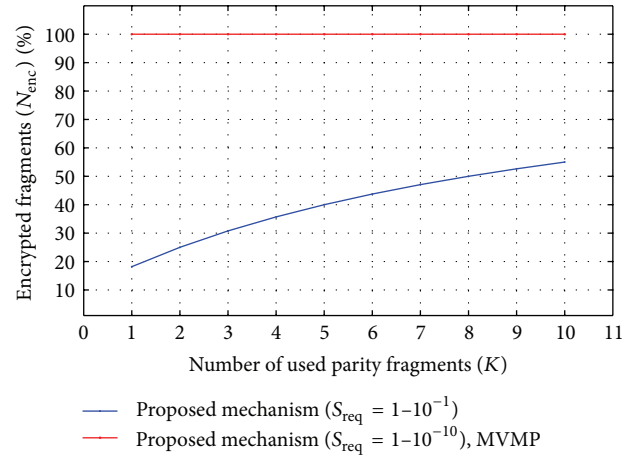


FIGURE 8: Percentage of encrypted fragments (N_{enc}) for a data packet of size $M = 10$ fragments.

encrypted. Note that encrypted packets influence encryption time and energy consumption; more encrypted fragments require more time and consume more energy.

6. Conclusions

In this paper, we propose and evaluate a secure and reliable routing protocol for WSNs that is designed to handle the application security requirements and reliable data transmission using coding and selective encryption scheme. In the proposed protocol, RS code is used to provide reliability and security. The proposed routing protocol is based on the node-disjoint multipath established depending on the link security parameters. The sink node decides on the paths selection process in order to satisfy the application requirements and the number of these paths is determined to enhance the security. Thus, different number of paths can

be used for different security requirements. A novel security mechanism is proposed to support secure data transmission while respecting the network restrictions in terms of energy. The protocol reduces the energy consumption at sensor nodes by moving the path selection process to the sink node. Moreover, reducing the number of encrypted packets based on the required level of security limits energy consumption. Using different paths for different security requirements to route data and permitting the sink to be responsible for the path selection process, attacks such as the Sinkhole and Wormhole are no longer related, where in a Sinkhole attack the attacker tries to attract the traffic of surrounding neighbors by making itself look attractive to the surrounding neighbors with respect to the routing metric, and in a Wormhole attack two or more attackers may establish better communication tunnels between them in the path.

References

[1] E. Stavrou and A. Pitsillides, "A survey on secure multipath routing protocols in WSNs," *Computer Networks*, vol. 54, no. 13, pp. 2215–2238, 2010.

[2] D. Kandris, M. Tsagkaropoulos, I. Politis, A. Tzes, and S. Kotsopoulos, "Energy efficient and perceived QoS aware video routing over wireless multimedia sensor networks," *Ad Hoc Networks*, vol. 9, no. 4, pp. 591–607, 2011.

[3] Y. Li, C. S. Chen, Y. Q. Song, and Z. Wang, "Real-time QoS support in wireless sensor networks: a survey," in *Proceedings of the International Conference on Fieldbuses and Networks in Industrial and Embedded Systems*, pp. 373–380, Toulouse, France, November 2007.

[4] 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.

[5] E. Felemban, C. G. Lee, and E. Ekici, "MMSPEED: multipath Multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 6, pp. 738–753, 2006.

[6] W. Lou and Y. Kwon, "H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 55, no. 4, pp. 1320–1330, 2006.

[7] W. Lou, W. Liu, and Y. Fang, "SPREAD: enhancing data confidentiality in mobile ad hoc networks," in *Proceedings of the IEEE 23th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '04)*, pp. 2404–2413, Hong Kong, March 2004.

[8] C. H. Shih, Y. Y. Xu, and Y. T. Wang, "Secure and reliable IPTV multimedia transmission using forward error correction," *International Journal of Digital Multimedia Broadcasting*, vol. 2012, Article ID 720791, 8 pages, 2012.

[9] M. Ruiping, L. Xing, and H. E. Michel, "A new mechanism for achieving secure and reliable data transmission in wireless sensor networks," in *Proceedings of the IEEE Conference on Technologies for Homeland Security: Enhancing Critical Infrastructure Dependability*, pp. 274–279, Woburn, Mass, USA, May 2007.

[10] H. Alwan and A. Agarwal, "A survey on fault tolerant routing techniques in wireless sensor networks," in *Proceedings of the 3rd International Conference on Sensor Technologies and Applications (SENSORCOMM '09)*, pp. 366–371, Athens, Greece, June 2009.

[11] A. D. Wood and J. A. Stankovic, "Poster abstract: AMSecure: secure link-layer communication in TinyOS for IEEE 802.15.4-based wireless sensor networks," in *Proceedings of the 4th International Conference on Embedded Networked Sensor Systems (SenSys '06)*, pp. 395–396, New York, NY, USA, November 2006.

[12] I. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society For Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, 1960.

[13] S. K. Singh, M. P. Singh, and D. K. Singh, "A survey on network security and attack defense mechanism for wireless sensor networks," *International Journal of Computer Trends and Technology*, vol. 1, no. 2, pp. 9–17, 2011.

[14] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[15] L. Chen and J. Leneutre, "On multipath routing in multihop wireless networks: security, performance and their Tradeoff," *Journal of Wireless Communication and Networking, EURASIP*, vol. 2009, Article ID 946493, 13 pages, 2009.

[16] Y. Challal, A. Ouadjaout, N. Lasla, M. Bagaa, and A. Hadjidj, "Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1380–1397, 2011.

[17] N. Nasser and Y. Chen, "SEEM: secure and energy-efficient multipath routing protocol for wireless sensor networks," *Computer Communications*, vol. 30, no. 11-12, pp. 2401–2412, 2007.

[18] J. Ben-Othman and L. Mokdad, "Enhancing data security in ad hoc networks based on multipath routing," *Journal of Parallel and Distributed Computing*, vol. 70, no. 3, pp. 309–316, 2010.

[19] W. Wang, D. Peng, H. Wang, and H. Sharif, "An adaptive approach for image encryption and secure transmission over multirate wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 9, no. 3, pp. 383–393, 2009.

[20] H. Alwan and A. Agarwal, "Multi-objective reliable multipath routing for wireless sensor networks," in *Proceedings of IEEE Globecom Workshop on Ad Hoc and Sensor Networking (GC '10)*, pp. 1227–1231, Florida, Fla, USA, December 2010.

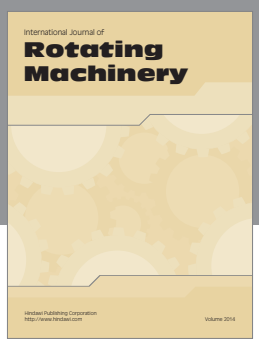
[21] H. Alwan and A. Agarwal, "A secure mechanism for QoS routing in wireless sensor networks," in *Proceedings of the 25th IEEE Canadian Conference on Electrical & Computer Engineering*, pp. 1–4, Montreal, Canada, April 2012.

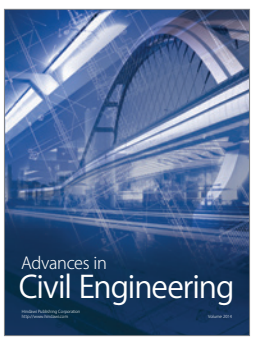
[22] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes," in *Proceedings of the 2nd ACM International Workshop on Wireless Sensor Networks and Applications (WSNA '03)*, pp. 151–159, San Diego, Calif, USA, September 2003.

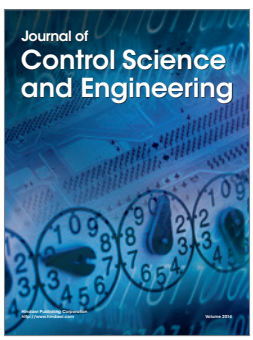
[23] H. Wang, M. Hempel, D. Peng, W. Wang, H. Sharif, and H. H. Chen, "Index-based selective audio encryption for wireless multimedia sensor networks," *IEEE Transactions on Multimedia*, vol. 12, no. 3, pp. 215–223, 2010.

[24] H. Alwan and A. Agarwal, "Multi-objective QoS routing for wireless sensor networks," in *Proceedings of the International Conference on Computing, Networking and Communications*, pp. 1074–1079, San Diego, Calif, USA, January 2013.

[25] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 4, pp. 11–25, 2001.







Hindawi
Submit your manuscripts at
http://www.hindawi.com