Research Article

Energy-Efficient Secure Path Algorithm for Wireless Sensor Networks

Imanishimwe Jean de Dieu, Nyirabahizi Assouma, Maniraguha Muhamad, Wang Jin, and Sungyoung Lee

Department of Computer Engineering, Kyung Hee University, Seoul 130-701, Republic of Korea

Correspondence should be addressed to Imanishimwe Jean de Dieu, jeanishimwe@oslab.khu.ac.kr

Received 19 June 2011; Accepted 16 January 2012

Academic Editor: Rajgopal Kannan

Copyright © 2012 Imanishimwe Jean de Dieu et al. 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.

To collect the data and transmit them on the base station is the main task of the sensor nodes in wireless sensor networks (WSNs). This transmission requires a specific routing algorithm. To prolong the network lifetime, sensor nodes need a secure load-balancing route. In this paper, we investigate the facts of ensuring secure sensed data in a balanced energy network backbone, and propose energy-efficient secure path algorithm (ESPA) for WSNs. It is a process of ensuring sensed data authenticity and integrity under a well-structured energy-efficient routing. To overcome the limitation caused by the symmetric key cryptography algorithms for securing data in WSNs, we proposed a mechanism for checking data integrity in a balanced energy network backbone. On this basis, we use the combined version of distance energy aware routing and a checking data integrity method for WSNs. ESPA provides a better performance in maximizing the network lifetime.

1. Introduction

Wireless sensor networks (WSNs) [1–3] are the most important technologies which are used in variety of applications. To impact these applications in real-world environments we need more efficient strategies to guarantee security on the sensor readings as well as to prolong or maximize the network lifetime. WSNs use tiny and inexpensive sensor node devices; these multifunctional miniature devices perform limited and also specific monitoring and sensing functions [4]. They permit very low energy consumption and have very low processing power as well as low radio ranges [1]. The sensor nodes will sense, process and then transmit the data to a certain remote sink node (base station) in an autonomous and unattended manner [4].

Secure sensor readings are important when confidential data are involved in WSNs applications [1, 5, 6]. WSNs pose unique challenges in terms of designing security mechanisms, specifically due to power, computation, and communication constraints of individual sensors. As WSNs are used in everyday life, the secure energy, efficient routing of monitored sensitive data becomes an important issue.

Our paper is mainly inspired by the work in [7] where the symmetric key (shared key) was used to ensure the protection of actual sensed data in WSNs. Their work was well analyzed in different challenges. However, symmetric key can be extracted by an attacker through a compromised node and without checking integrity on the receiver side; this may result on delivering a modified data to a base station (BS).

In this paper, we present an energy-efficient secure path algorithm (ESPA) for wireless sensor networks which aims to achieve authenticity and integrity on the actual sensed data within an energy-efficient network infrastructure. Due to inherent deployment nature and energy limitation constraint of the sensors, ensuring energy efficiency together with the security of the sensed data becomes a foremost task [8]. Our scheme ensures the secure transmission of data from the source sensors to the base station in a way that it can consume the available amount of energy in a balanced manner after selecting an optimal path within the whole network. We use one-way hash function and shared secret keys for ensuring security service on the sensed data. In ESPA, a routing architecture is created as the topology of the network. The key contribution in this paper is to ensure secure transmission...
which results prolonging network lifetime via a suboptimal energy-efficient and balancing routing algorithm. Below a list of achievement is shown.

1. In multipath routing, we first select the shortest path based on an ant-colony optimization method adopted in WSNs.

2. Based on the selected path, the traffic load will be balanced from a source node to base station based on the optimal distance of each node to base station. This will increase the lifetime of the whole network.

3. The privacy of the sensor readings will be achieved through a service of anonymity which results hiding the source node identity along the transmission path and only the base station will identify the sender.

4. On the packet delivery along the path from source, node to base station node symmetric key and hash function will defend an attack vector, and more strong verification will be done on the receiver side (base station) to guaranty the authenticity and integrity of the actual sensed data.

5. Simulation results and comparisons are provided with a scenario application for healthcare.

The rest of the paper is organized as follows. Section 2 introduces some related work of energy efficient and secure routing algorithms. In Section 3 we present the motivation of our work. In Sections 4 and 5, the details of our ESPA are described based on the theoretical and numerical analysis under different models. Performance evaluation and comparison are given in Sections 6 and 7 concludes this paper.

2. Related Work

Transmission between the end nodes can occur in a single hop, or up to N hops [6]. Many existing researchers indicate that on multihop routing more short hops are preferable to fewer long hops, because the minimum signal-to-noise ratio (SNR) along the route is larger for multihop. But as indicated in [9] this consideration does not take into account the important practical issues of resource allocation, end-to-end delay, error propagation, and interference induced by extra transmissions. Therefore, a new routing method should be adapted to prevent routing over many short hops. In [10], a hierarchical structured energy efficient routing protocol called LEACH is presented, it is a smart solution where clusters are formed to merge data before transmitting to the base station. By using the cluster heads chosen to transmit to the base station, LEACH achieves a factor of 8 improvement compared to direct transmissions and the energy consumption is balanced via the rotation of 5% cluster heads and it is greatly reduced by data aggregation inside each cluster head. However, clustering will require more energy during rotation of cluster heads.

In [11], an energy-efficient routing schemes for wireless sensor networks is proposed where after making a study on energy-optimal network configurations for manual and random placement of nodes under a natural coverage criterion; they proved that, in a linear network, energy consumption is minimal when nodes are equally spaced. However, the load is not equally to all the nodes therefore energy distribution should take into account the traffic load from the source to destination.

Energy-efficient secure pattern based data aggregation for wireless sensor networks ESPDA is presented in [12] which focused on the issue of energy-efficient data aggregation with secure data transmission. ESPDA keeps the data transmission and aggregation more secure by limiting the cluster heads to decrypt or encrypt the data received from the sensor.

In [8], secure energy-efficient routing protocol for densely deployed wireless sensor networks SERP is presented which aims to achieve robust security for transmitted sensor readings with an energy-efficient backbone. They proposed a network routing model which aims at minimizing the wasteful energy consumption by energy-efficient structuring of the network and then security on the sensed data transmissions from the sensors to the base station using one-way hash chain and shared secret keys. Their routing model selects a minimum number of forwarding nodes in the network through energy- and distance-based efficient structuring of the network which helps for maximizing the lifetime of the network. However, these exchange control messages will introduce more control overheads as well as require more energy consumption and for security defense mechanism the identity of the source node is publicly known, therefore, brute-force search and eavesdropping attacks are free to gain access on the system.

The energy efficient ant based routing algorithm for WSNs (EEABR) [13], based on an ACO metaheuristic, is a proposed ant-based algorithm to maximize the lifetime of WSNs. The algorithm uses a good strategy considering energy levels of the nodes and the lengths of the routed paths.

Even though the above-mentioned energy-efficient and secure routing protocols or algorithms can improve prolong network lifetime to some degree, they cannot effectively overcome the burden overhead in communication known as hotspot problem which is tightly related with energy and traffic models. In this paper, we propose a load balanced distance-based energy aware routing algorithm which can effectively alleviate the hotspot problem based on the theoretical deduction and analysis of relevant models. Under this well-designed route, the packet will be delivered to the destination in a secure manner with help of a keyed hash function.

3. Problem Statement

WSNs are one of the most important technologies which are used in a variety of applications. To impact these applications in a real-world environment, we need more efficient strategies to guarantee secure communication on the sensor readings as well as to maximize the whole network lifetime. Since the sensor nodes are equipped with limited energy batteries, the energy conservation is the primary challenge for WSNs.

On this basis, the energy efficient information processing is of critical importance to balance the available residual
amount of energy and to operate the deployed networks as long as possible. The objective of prolonging the network lifetime is not only to reduce energy consumption during the sensing, processing, or control processes, but also to balance energy consumption among the sensor nodes. If some sensor nodes die early, the whole network will quickly get partitioned and out of function, for example in the case of hotspot problems. Wherein, under a multipath routing, nodes closer to the base station (BS) die early, while in a direct transmission routing, nodes far from the BS die early.

Many schemes have been proposed using a symmetric key cryptography algorithm for securing data in WSNs. However, a current limitation of these schemes is that the symmetric key cryptography algorithms are vulnerable to node compromise attacks. To overcome this limitation, we propose a scheme for ensuring secure sensed data in a balanced energy network backbone from the source node to base station. Therefore, this motivated our work in this paper. We deal with the issue of balancing the available residual energy of the whole network infrastructure and guarantee that the packet data is delivered under a well secured route.

4. Proposed Approach

4.1. Network Model. The proposed approach for ensuring data privacy protection in WSNs through an energy-efficient network backbone is comprised of two phases. At the first phase, we proposed a distance based energy aware routing (DEAR) algorithm on selected optimal path through Ant colony optimization (ACO). The objective of this phase is to balance the available amount of energy in the whole WSNs as well as to maximize the network lifetime. At the second phase in the proposed network routing we ensured confidentiality, authenticity, and integrity security services on the sensed data. Figure 1 shows the complete architecture of the proposed model. ACO will be adopted for searching an optimal path from the source node to the base station. The reason of choosing ACO is due to its distributed nature and quick reaction to changes in the network.

There are a number of reasons that ACO algorithms are a good fit for WSN routing. ACO algorithms are decentralized just as WSNs are similarly decentralized. In WSNs nodes can break, run out of energy and have the radio propagation characteristics change. ACO algorithms have been shown to react quickly to changes in the network [14].

There are two types of packets in our approach: data packets and ant (or control) packets. Data packets are the data carried in the sensor network. The routing algorithm routes these packets from the source to the destination, but has no interest in the contents of these packets. Forward and backward ants named ACO\textsuperscript{F} and ACO\textsuperscript{B}, respectively, are represented by control packets. These packets are used to update the routing table.

Information or results from control packets will be stored in a Path\textsuperscript{info} repository. Path\textsuperscript{info} repository is required to maintain or store all available optimal selected results and send them to DEAR (distance energy aware routing) on the event based for load balancing. When the event boost the initialization has to be sent on ACO to initiate the already obtained optimal path. The actual sensed data will be sent under the control of DPP (data privacy protection) for protecting the sensory data readings from malicious.

Sensor will then send the obfuscated collected data via a well-selected path to a command center known as the base station or sink. The DPP verification process will be performed for ensuring the authenticity and integrity on the actual sensed data. Therefore, the packets will be accepted or dropped according to a verification process.

In wireless sensor network, there are so many challenges. The main challenges are how to provide maximum lifetime to the network and how to provide secure communication to the network. As sensor networks totally rely on battery
power, the main aim for maximizing the lifetime of the network is to conserve battery power or energy with some security considerations. Our algorithm is suitable to the model as follows

(i) The bidirection link is used in networks. That is to say, if sensor A can communicate with sensor B, then sensor B can communicate with sensor A.

(ii) The initial energy in sensors is equal. During the early period of the network’s life, there is enough energy in sensors to communicate with border sensors.

(iii) The sensor has an all-direction antenna.

4.2. Sub optimal Selection Phase. In our scheme, the first phase is to build a suboptimal path among available multi-path routes through an ACO, based technique. On this basis, each ant tries to find a path in the network by providing minimum cost. Ants are initiated from a source node s, move through neighbor nodes ri, and reach a final destination node (base station). As shown in (1), the choice of the next node r is made according to a probabilistic decision rule proposed in the ACO metaheuristic [14]:

\[
p_k(r, s) = \begin{cases} 
\frac{[\tau(r, s)]^\alpha \times [\eta(r, s)]^\beta}{\sum_{r \in R_s} [\tau(r, s)]^\alpha \times [\eta(r, s)]^\beta} & \text{if } r \notin \text{Mem}_k, \\
0 & \text{otherwise},
\end{cases}
\]

(1)

where \( \tau \) is the routing table at each node that stores the amount of pheromone trail on connection \((r, s)\) \cdot \( \eta \) is the visibility function. \( R_s \) is the receiver nodes and \( \text{Mem}_k \), is the list of identities of every visited node, which is carried by ant \( k \).

During ant’s exploration, forward ant (ACO_F) will collect all the information of the paths passed by, while backward ant (ACO_B) recoiling back from a destination node (base station) to a source node s. During its moving back, ACO_B will update the routing tables of all the nodes along the path according to the information collected by the corresponding ACO_F. Each ant has the memory which contains the already visited nodes, by exploiting this ant’s memory; an ant \( k \) can build feasible solutions. On this, no node can be visited more than once, which is shown by the Figure 2. At each node \( r \), a forward ant selects the next hop node using the same probabilistic rule proposed in the ACO metaheuristic [14]. The visibility function is given by

\[
\eta = \frac{1}{e_i - \bar{e}_i},
\]

(2)

where \( e_i \) is the initial energy level of the nodes and \( e_i \) is the current energy level of the node s. This enables decision making according to neighbor node’s energy levels, meaning that if a node has a lower energy source then it has lower probability to be chosen. Nodes inform their neighbors about their energy levels when they sense any change in their energy levels. Here, \( a \) and \( \beta \) are parameters that control the relative importance of trail versus visibility. In this case, probability selection is based on two important factors: the energy and pheromone intensity; whereby the nodes with more energy should be chosen with high probability and if on connection \((r, s)\) there has been a lot of traffic then it is highly desirable to use that connection.

Once a forward ant reaches the destination node, it is transformed in a backward ant with the aim of updating the pheromone trail of the path it used to reach the destination and that is stored in its memory. This update will be computed by the destination node through this formula

\[
\Delta \tau = \frac{1}{N - F_{dk}},
\]

(3)

where \( N \) is the number of nodes stored in the ant’s memory and \( F_{dk} \) is the distance travelled by the forward ant \( k \). When the backward ant reaches the node where it was created, its mission is finished, and the ant is eliminated. The path with more pheromone intensity will indicate the shortest route and then, a suboptimal path will be obtained.

4.3. Energy-Balancing Phase. From Figure 2, our scenario shows that when an event occurs in WSNs, the source node will transfer the data to the base station (BS) in two phases: Direct transmission routing “single hop” when the sensor node is located near the base station and multihop routing when the source node is located far away from the sink node. As proposed in our previous work [4], for direct transmission routing, the nodes far away from sink node will drain out of energy very quickly due to the characteristics of wireless channel. For multihop routing, the nodes close to sink node will have more traffic load to forward under most routing mechanisms and also drain out of energy quickly.

Table 1 shows the energy distribution along the network from the source node to base station by considering 4 nodes to reach the sink. On the event based scenario refer to Table 1, each node will require one round of an amount of energy to transmit \( E_{FS} \) its own message and the round time for forwarding the message from previous nodes, it will increase one round per hop on the path towards the base station and this will results on more energy forwarding \( E_{FS} \) consumption for the nodes closer to the sink (base station). Distance based energy balancing scheme is proposed to deal with this problem as well as maximizing the network lifetime.
Table 1: Round traffics.

| Sensors | Transmit | Forward |
|---------|----------|---------|
| S1      | 1        | 0       |
| S2      | 1        | 1       |
| S3      | 1        | 2       |
| S4      | 1        | 3       |

Algorithm 1 clearly shows the basic steps for distance-based energy aware routing: “this algorithm is used for balancing the energy in a whole network as well as maximizing the network lifetime.” Where $\propto$ is the energy attenuation power parameter related to a specific field, $d$ is the distance between the sender and receiver. However, the distribution is not far from uniform, as manifested by the small variance of $d$. For $E_{\text{elec}} = 10$, and $\propto = 2$, the variance is about 0.14. For $\propto = 3; 4$, the variances are 0:058, 0:029, the gain in total energy consumption varies between 22% ($\propto = 4$) and 28% ($\propto = 2$). The gain in lifetime is considerably higher and ranges between a factor of 2.3 ($\propto = 4$) and 2.5 ($\propto = 2$).

Iteratively other nodes also repeat the same process. Under one dimensional linear network, sensor nodes are usually placed in a line from source node to a base station node.

$$E_{Tx}(l, d) = \begin{cases} \frac{1}{2}E_{\text{elec}} + l \cdot \varepsilon_{f_i} \cdot d^2, & \text{if } d < d_0, \\ \frac{1}{2}E_{\text{elec}} + l \cdot \varepsilon_{\text{mp}} \cdot d^4, & \text{if } d \geq d_0, \end{cases}$$

$$E_{Rx}(l) = \frac{1}{2}E_{\text{elec}},$$

$$E_{Fx}(l, d) = E_{Tx}(l, d) + E_{Rx}(l),$$

where $E_{Tx}$ The amount of energy to transmit $l$-bits messages over a distance $d$, $E_{Rx}$ amount of energy to receive the message and $E_{Fx}$ amount of energy to forward the message. For other parameters, $E_{\text{elec}}$ is the Energy dissipation to run the radio device, $\varepsilon_{f_i}$ free space model of transmitter amplifier, $\varepsilon_{\text{mp}}$ multipath model of transmitter amplifier, and $d_0$ the distance threshold.

In this section, we present our improved version of ensuring the least energy consumption through a load balanced routing based on an obtained suboptimal path from the previous section. Here, our objective is to balance the load along the path from the source node to the base station node. An individual distance from one node to next hop node is computed and the energy will be consumed at the similar rate.

Basically, we are targeting to get the optimal multihop number and each individual distance $d_i$ so that each node consumes the least energy at similar rate. Based on (4), the total energy consumption to transmit one bit data ($l = 1$) over $n$-hop route will be

$$E(n) = \left( E_{\text{elec}} + \varepsilon_{\text{amp}} \cdot d_i^a \right) + \sum_{i=2}^{n} \left( 2E_{\text{elec}} + \varepsilon_{\text{amp}} \cdot d_i^a \right)$$

$$= (2n - 1)E_{\text{elec}} + \sum_{i=1}^{n} \varepsilon_{\text{amp}} \cdot d_i^a.$$  

Therefore, $E(n)$ is finally equal to

$$E(n) = (2n - 1) \cdot E_{\text{elec}} + \varepsilon_{\text{amp}} \cdot n^{1-a} \cdot d^a. \quad (6)$$

As the (5) has a minimal value when $d_1 = d_2 = \cdots = d_n = d/n$. Then, our minimum point can be obtained through the first derivative of (6). In this case we can get

$$2E_{\text{elec}} + \varepsilon_{\text{amp}} \cdot (1 - \alpha) \cdot \left( \frac{d}{n} \right)^a = 0 \quad (7)$$

Therefore, we can get $E_1 \approx E_2 = E_3 \cdots = E_n$.

In this case, all involved sensors will consume their energy at similar rate, which can effectively alleviate the hotspot problem and prolong the network lifetime.

We are also considering the second case where on the whole network, the packet or traffic length is not the same, in this scenario a certain node which is the furthest from the base station only needs to transmit its data once while other node $n$ which is closest to base station has to transmit its own data once and help forward the data $(n-1)$ times along the line. On this basis, the node $n$ will become a hotspot node as it has a lot of burden to forward and then die quickly.

Let us consider that a node $i$ will transmit its own data and help to forward other traffics for $(i-1)$ times. Here, the energy consumption for node $i$ is

$$E_i = l \cdot \left( E_{\text{elec}} + \varepsilon_{\text{amp}} \cdot d_i^a \right) + l \cdot (i - 1) \left( 2E_{\text{elec}} + \varepsilon_{\text{amp}} \cdot d_i^a \right)$$

$$= l \cdot (2i - 1)E_{\text{elec}} + l \cdot i \cdot \varepsilon_{\text{amp}} \cdot d_i^a. \quad (8)$$

Since our objective is to let each node consume the energy at similar rate, then $E_i = E_{i+1}$, we can get

$$l \cdot \left( (2i - 1)E_{\text{elec}} + i\varepsilon_{\text{amp}}d_i^a \right) = l \cdot \left( (2i + 1)E_{\text{elec}} + (i + 1)i\varepsilon_{\text{amp}}d_{i+1}^a \right), \quad (9)$$

$$\begin{align*}
(i + 1)i\varepsilon_{\text{amp}}d_{i+1} &= (2i - 1)E_{\text{elec}} + i\varepsilon_{\text{amp}}d_i^a - (2i + 1)E_{\text{elec}},
(i + 1)i\varepsilon_{\text{amp}}d_{i+1} &= -2E_{\text{elec}} + i\varepsilon_{\text{amp}}d_i^a,

d_{i+1} &= \frac{-2E_{\text{elec}} + i\varepsilon_{\text{amp}}d_i^a}{\varepsilon_{\text{amp}}(i + 1)},
\end{align*}$$

$$d_{i+1} = \sqrt{\frac{-2E_{\text{elec}} + i\varepsilon_{\text{amp}}d_i^a}{\varepsilon_{\text{amp}}(i + 1)}}. \quad (10)$$

From (10), we can deduce

$$d_i^a = \frac{-2E_{\text{elec}} + (i - 1)i\varepsilon_{\text{amp}}d_{i-1}^a}{i\varepsilon_{\text{amp}}}. \quad (11)$$

Here, we can notify that

$$i\varepsilon_{\text{amp}}d_i^a = -2E_{\text{elec}} + (i - 1)i\varepsilon_{\text{amp}}d_{i-1}^a. \quad (12)$$

We substitute this in (11), then

$$d_{i+1} = \sqrt{\frac{-2(2E_{\text{elec}} + (i - 1)i\varepsilon_{\text{amp}}d_{i-1}^a)}{\varepsilon_{\text{amp}}(i + 1)}}. \quad (13)$$
Load Balancing

**Input:** sensor nodes, distance form each sensor node to base station, base station address and distance to neighbor nodes

**Output:** Maximizing network lifetime through bes routing

1. /* calculate optimal distance value, where
   \( a \in [2, 4] \)
   \( \epsilon_{\text{amp}} = \epsilon_{\text{elec}} \) when \( \alpha = 2 \) and
   \( \epsilon_{\text{amp}} = \epsilon_{\text{imp}} \) when \( \alpha = 4 \).
   */
   
   \[ d_i = \frac{2 \cdot E_{\text{elec}}}{\epsilon_{\text{amp}}(\alpha - 1)} \]

2. /* neighbors selection */

3. /* calculate distance from source neighbors */

4. /* compare optimal distance \( d_i \) with \( d_i^{\text{opt}} \) */

5. Finally;

6. End

Algorithm 1: Distance-based network model.

From (13), we can get

\[
\begin{align*}
\ell_{i-2}^n &= -\frac{2E_{\text{elec}} + (i-2)\epsilon_{\text{amp}}\ell_{i-2}^n}{(i-1)\epsilon_{\text{amp}}} = (i-1)\epsilon_{\text{amp}}\ell_{i-2}^n + E_{\text{elec}} \quad \text{(14)}
\end{align*}
\]

By substituting this in (13), then

\[
\ell_{i+1}^n = \sqrt{\frac{-2E_{\text{elec}} + (i-2)\epsilon_{\text{amp}}\ell_{i-2}^n}{\epsilon_{\text{amp}}(i+1)}} \quad \text{(15)}
\]

Iteratively, then we can get

\[
\ell_{i+1}^n = \sqrt{\frac{-2E_{\text{elec}} + \epsilon_{\text{amp}}\ell_{i}^n}{\epsilon_{\text{amp}}(i+1)}} \quad \text{(16)}
\]

Since the individual distance \( d_i \) is always positive then:

\[ (-2(n-1)E_{\text{elec}} + \epsilon_{\text{amp}}d_i) / \epsilon_{\text{amp}}(n) > 0 \]

then from this equation we can deduce:

\[ -2nE_{\text{elec}} > -\epsilon_{\text{amp}}d_i^2 - 2E_{\text{elec}} \]
\[ 2nE_{\text{elec}} < \epsilon_{\text{amp}}d_i^2 + 2E_{\text{elec}} \quad \text{(17)} \]

thus it proves that: \( n < (\epsilon_{\text{amp}}d_i^2 / 2E_{\text{elec}}) + 1 \), and from here, we can also deduce the corresponding lower bound distance when hop number \( n \) is known:

\[ d_i^2 > \frac{2(n-1)E_{\text{elec}}}{\epsilon_{\text{amp}}} \quad \text{(18)} \]

On the other hand, given the minimal distance from the source node to base station \( d_i \), there might be several multi-hop routes with different hop number \( n \). On this basis, we first select the suboptimal route path by using ant-colony optimization technique and then on that chosen route, we select the highest hop number above with the minimal energy consumption for each sensor node and this is the optimal multi-hop number we need.

Therefore, from the above analysis, we can conclude that:

Given the source to base station node distance \( d_i \) and the suboptimal route among available routes, the optimal multi-hop number \( n \) as well as each individual distance \( d_i, i \in [1, n] \) can be determined so that all the sensor nodes consume their energy at similar rate.

Below pseudocodes for suboptimal balanced route are shown, in each searching period, an ant \( a_i \) chooses a path randomly according to a predetermined path selection possibility. An optimal path searching period ends up in the algorithm when all the \( n \) ants finish the path seeking respectively.

Load Balancing under an Optimal Path. See Algorithm 2.

After obtaining \( d_i \) as a selected suboptimal path and then the sensed data will be directly sent or forwarded through this path under an individual optimal distance to reach the next forward node and so on till the base station.

5. Control Point Checking Phase

Our proposed secure path solution ensures authenticity and integrity of the actual sensed privacy in WSNs by providing a checking mechanism on the receiver side (base station). This will provide the evidence that the packet has reached the destination without being modified along the path. Here, our first stage is to claim the weak point of symmetric key, which is usually known as a single point failure based on a single shared key. On this basis, the symmetric key may be captured by en-route attack. Therefore, data integrity checking on the receiver side is needed through a hashing operation by ensuring that the packet received was un-altered during its transmission from a source to destination by any intermediate sensor or malicious node. Below Figure 3 is the proposed secure model.

5.1. Sender Side

5.1.1. \( E(ID_s || R_n, K_{mp}) \). Here, we apply concatenation between the source sensor ID and random number \( R_n \) (with
the same size as the sensor identity) in order to provide protection against brute-force search attacks and then we encrypt them with \( K_{bs} \) (public key of the base station (receiver)) to provide anonymity of the source node against some attacks from attack vector.

5.1.2. \( E(Data) \), \( K_{x,BS} \). Secondly, we encrypt the sensed data with \( K_{x,BS} \) symmetric key shared between sender and base station (receiver), as secrecy of actual sensed data for providing confidentiality.

5.1.3. \( E(Data) \), \( K_{x,BS} \). Next, we apply one-way hash function on the sensed data and to enhance data security we also encrypt the message digest by the symmetric key (shared secret key between the source node and the base station). To reach our goal of ensuring authenticity and integrity on the sensor readings from the source to destination; we concatenate the cipher-text obtained in the previous step with the later result that becomes \( E(data, K_x, bs) \ || \ E(H(Data)), K_x, bs) \).

5.2. Receiver Side

5.2.1. \( D(ID_x \ || \ R_n, K_{x,BS}^* \). Decryption to get source node identity (ID) by using the private key of the base station.

5.2.2. Integrity and Authentication Verification. After separating the cipher text data \( E(Data) \) and the cipher text message digest \( E(H(Data)) \) both will be decrypted by using shared secret key between the source node and the base station. Next, we save the plain-text message digest and then one-way hash function will be applied on the plain-text data obtained and finally we compare the result. Thus, the overall process results on checking data integrity to ensure that during the transmission from the source node to destination (base station) the packet has not been modified and authenticate that the packet has been sent by legitimate user.

In this paper, our security scheme is built based on the assumption that the gateway or base station is a central command authority. It has no resource constraint problem, and furthermore it cannot be compromised by an attacker. In order to provide protection against en-route attacks from traffic analysis or fabrication during transfer from one node to another, we propose a secure communication model, which can be established with the help of hybrid key (asymmetric key and symmetric keyed hash function) scheme. On this basis, asymmetric key (between the sensor node and the base station) is used only for hiding the sensor node identity (anonymity), which results on identity privacy. While the symmetric keyed hash function is used to protect the whole actual sensed data.

If an adversary compromises a sensor node, he cannot successfully deceive the base station to perform insider...
attacks, due to the infeasible computational properties of keyed hash functions. This makes it extremely difficult for an adversary to retrieve the necessary keys to decrypt or gain access to the original message. This also provides a simple resistance in the case of nodes compromising, as the key established between non-compromised nodes remains confidential.

Our scheme is also resilient to the second type of node compromised, where an attacker injects the nodes in the network with the false identities. In this case, the base station will be able to detect this attack through a failure verification of our anonymity mechanism.

If an insider attack (from a compromised node) gets the packet from that compromised one, it could use the last shared key to access the data, and then, the false packet could be sent successfully to the base station. In this case, the false packet will be composed by two concatenated contents: fake data and genuine message digest. Therefore, the base station verification will indicate the attacker failure point through an authentication failure.

6. Performance Evaluation

6.1. Security Analysis. We analyze the security of our scheme with respect to two goals: the ability of the base station to detect an altered message and the ability of the source node to mask its identity (id) for data privacy issue.

In this scheme, the data packet is transmitted under the keyed hash function covered by the shared key $K_{x,BS}$ between the sensor node and the base station. Hence, the shared key $K_{x,BS}$ is never disclosed during transmission. The shared key $K_{x,BS}$ is only known by the related peers, that is, the sensor node and the base station.

An eavesdropper at the edge of the sensor node fails to monitor or capture the random number $R_n$ as well as the identity of the sensor node based on hiding features from the asymmetric key $K_{BS}$. On this basis, without a proper matching of those dual keys (public key of the base station and private key of legitimate sensor node), any malicious node will not gain access to the context information or being able to forward the packets to next nodes. Therefore, this
attribute could prevent camouflage and traffic attacks and be useful to protect sensor node privacy.

The data packets from the sensor node to the base station are authenticated by a keyed hash function. Before accepting the inward packet data and making further processing, the receiver must verify the authentication. Based on the infeasible computational properties of a hash algorithm, the base station and sensor node could avoid the attacks of denial of service. According to the above analysis, this proposed scheme, which is simple and easy to implement, can provide relatively strong protection for sensor node networks.

6.1.1. Base Station Verification Theoretical Analysis. An attacker can utilize devices with the same capabilities as the sensor nodes in the network, either by introducing sensor nodes to the networks deployment area or by destroying some of the nodes in the network under attack.

Assume that an adversary \( j \) has known the secret key (shared) between source node and base station. \( j \) will have access to the concatenated data between message digest and actual sensed data. As only base station has the knowledge of the size of the cipher text \( (E[h(data), K_{s,BS}]) \), therefore, \( j \) will not be able to separate the concatenated payload. If so, then the data will be stolen or only modified according to what kind of attacker, but as one-way hash function has following properties

(a) \( H(x) = h \); where \( h \) equals to the result of one-way hash function of the message \( x \). So given \( h \), it is infeasible to find \( x \) (one-way property),

(b) \( H(x_1) = H(x_2) \) given \( x_1 \) is infeasible to find \( x_2 \) (weak collision resistance),

(c) \( H(x_1) = H(x_2)\), it is infeasible to find any \( x_1 \) and \( x_2 \) (strong collision resistance).

Therefore, the infeasible computational properties of a one-way hash function will help our scheme to identify any change that has occurred on the actual sensed data during the transmission from the source node to the base station. Thus integrity and authenticity will be achieved. To the best of our knowledge, ESPA can be able to defend against an outsider and insider attackers by adopting the knowledge of carrying out both cryptography and signature verification. With an outsider attack, an attacker does not become part of the network. An outsider attacker can choose to passively eavesdrop on the network communication, which is very difficult to detect. However, using a sufficiently strong cipher from hybrid key cryptography (asymmetric and symmetric) to preserve confidentiality is generally the only defense needed against this type of attack.

6.1.2. Base Station Verification Simulation Analysis. In our simulation, 5 to 16 packets per second (pps) were generated by the attackers to drainout energy of the nodes. When the packet authentication method is employed, the base station can detect false packets. In Figure 4, we show the number of alive nodes versus simulation time by considering our proposed authenticity checking mechanism. The graph shows that, if BS verification method is absent, the nodes lose the energy rapidly, which results in a shorter network lifetime.

If an insider attack (from a compromised node) gets the packet from that compromised one, it could use the last shared key to access the data, and then, the false packet could be sent successfully to the base station. In this case, the false packet will be composed by two concatenated contents: fake data and genuine message digest. Therefore, the base station verification will indicate the attacker failure point through an authentication failure.

6.2. Comparison Analysis. We compared our results with some existing schemes EEABR, SERP, and ESPDA based on evaluating the energy efficiency and security analysis issues. For performance evaluation, we use MATLAB software. As is shown in Table 2, there are 300 sensor nodes randomly deployed in a \( 300 \times 300 \text{ m}^2 \) area WSN with BS placed in the middle of the area. The maximal transmission radius is 150 meters. Each node takes turns to transmit a 2,000 bits message to BS using either direct transmission or multihop transmission based on different routing algorithms.

![Number of alive nodes per time](image)

**Figure 4: Number of alive nodes per time.**

| Table 2: Simulation parameters. |
|--------------------------------|
| **Parameter**                   | **Value**                   |
| Network size                    | \( 300 \times 300 \text{ m}^2 \) |
| Node number                     | 70–300                      |
| Radius                          | 150 m                       |
| Data length                     | 2,000 bits                  |
| Initial energy                  | 2 Joule                     |
| \( E_{elec} \)                  | 50 nJ/bit                   |
| \( \varepsilon_{mp} \)          | 0.0013 pJ/bit/m^4           |
| \( \Delta \)                    | [20, 50] m                  |
| BS                              | Inside or outside           |
| Sleep mode energy               | 0                            |
| Multipath model of transmitter amplifier (\( \varepsilon_{mp} \)) | 0.0013 pJ/bit/m^4           |
| Free space model of transmitter amplifier (\( \varepsilon_{fs} \)) | 10 pJ/bit/m^2               |
| \( \varepsilon_{mp} = \varepsilon_{mp} \) | \( \alpha = 4 \)             |
Figure 5 shows the average remaining energy under our infrastructure after dividing the number of nodes by the total area to get the network densities. In the simulation, the nodes close to the phenomenon send the actual sensed data through the neighbor nodes to the base station by consuming energy. The average remaining energy of the nodes decreases based on the incremental of the packets number received by the base station, Figure 5 gives the whole picture of the scenario. In the simulations, the proposed approach gives better results, by allowing each node to consume the least energy at similar rate.

In the simulation, the nodes close to the phenomenon send the actual sensed data through the neighbor nodes to the base station by consuming energy. The average remaining energy of the nodes decreases based on the incremental of the packets number received by the base station, in below Figure 5 gives the whole picture of the scenario. In the simulations, the proposed approach gives better results, by allowing each node to consume the least energy at similar rate.

We also analyze and evaluate the proposed secure model capability, with respect to three defense parameters: anonymity, confidentiality, and integrity, to determine the performance of our scheme. The possibility of defending an attack, $D_a$, depends on three factors: number of in-action nodes, failure verification, and our malicious counter threshold $\nu$:

$$D_a = \sum_{i=0}^{n} \binom{n}{i} (1 - I_f)^{\nu} I_f^{n-\nu}.$$  (19)

We defined $n$ as the number of observed nodes and $I_f$ as the interference factor occurring in a transmission tunnel. As shown in Figure 6, the performance of the proposed scheme depends on the incremental of in-action nodes, due to the interference factor caused by the packet collisions.

When the number of in-action nodes (sender and forwarder) increases, the number of receiving packets on the base station also increases. On this basis, our ESPA performs better checking results than SERP and ESPDA schemes, exceeding over 84% of dropping misbehavior packet.

7. Conclusions

To extend the network lifetime, we proposed an energy-efficient secure path algorithm for WSNs. The algorithm used distance-based energy-aware routing and data privacy protection techniques in WSNs. Using both techniques helped to improve the performance analysis of the system while achieving at the same time a good level of security in terms of authenticity and integrity of the sensed data, as well as maximizing the network lifetime. During the routing process, we tried to let each node to consume the least energy at similar rate under a suboptimal path.

In our future work, we plan to extend our work based on the implications of adopting a hybrid security scheme to handle storage and communication security, in order to implement the full confidential data privacy and how the algorithm can be used to achieve better performance.

Acknowledgment

This research was supported by the MKE (The Ministry of Knowledge Economy), Republic of Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National Industry Promotion Agency) (NIPA-2010-(C1090-1021-0003)).

References

[1] M. Li and Y. Liu, “Rendered path: range-free localization in anisotropic sensor networks with holes,” Proceedings of the ACM MobitCom, Published in IEEE/ACM Transactions on Networking (TON), vol. 18, no. 1, pp. 320–332, 2010.
[2] M.-S. Hwang and C.-Y. Liu, “Authenticated encryption schemes: current status and key issues,” International Journal of Network Security, vol. 1, no. 2, pp. 61–73, 2005.
[3] Y. Ouyang, Z. Le, J. Ford, and F. Makedon, “PrivaSense: providing privacy protection for sensor networks,” The ACM Conference on Embedded Networked Sensor Systems (SenSys ’07), vol. November 2007, no. Sydney, Australia.
[4] J. Wang, I. J. de Dieu, A. De Leon Diego Jose, S. Lee, and Y.-K. Lee, “Prolonging the lifetime of wireless sensor networks via hotspot analysis,” in Proceedings of the 10th annual International Symposium on Applications and the Internet (SAINT ’10), pp. 383–386, Seoul, Korea, July 2010.

[5] A. T. Campbell, S. B. Eisenman, N. D. Lane, E. Miluzzo, and R. A. Peterson, “People centric urban sensing,” in Proceedings of the 2nd annual International Wireless Internet Conference (WiCON ’06), pp. 18–32, August 2006.

[6] M. Sikora, J. N. Laneman, M. Haenggi, D. J. Costello, and T. Fujita, “On the optimum number of hops in linear wireless networks,” in Proceedings of the IEEE Information Theory Workshop (ITW ’4), pp. 165–169, October 2004.

[7] R. A. Shaikh, H. Jameel, B. J. d’Auriol, H. Lee, S. Lee, and Y. J. Song, “Achieving network level privacy in wireless sensor networks,” Sensors, vol. 10, no. 3, pp. 1447–1472, 2010.

[8] A. S. K. Pathan and C. S. Hong, “SERP: Secure energy-efficient routing protocol for densely deployed wireless sensor networks,” Annales des Telecommunications/Annals of Telecommunications, vol. 63, no. 9-10, pp. 529–541, 2008.

[9] M. Haenggi, “Twelve reasons not to route over many short hops,” in Proceedings of the IEEE 60th Vehicular Technology Conference, VTC2004-Fall: Wireless Technologies for Global Security (VTC ’04), pp. 3130–3134, Los Angeles, Calif, USA, September 2004.

[10] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-efficient communication protocol for wireless sensor networks,” in Proceedings of the The 33rd Annual Hawaii International Conference on System Sciences (HICSS-33), pp. 1–10, Hawaii, USA, January 2000.

[11] M. Khan, G. Pandurangan, and B. Bhargava, “Energy-efficient routing schemes for wireless sensor networks,” Tech. Rep. CSD TR 03-013, Department of Computer Science, Purdue University, West Lafayette, Ind, USA, 2003.

[12] H. Çam, S. Özdemir, P. Nair, D. Muthuvinashiappan, and H. Ozgur Sanli, “Energy-efficient secure pattern based data aggregation for wireless sensor networks,” Computer Communications, vol. 29, no. 4, pp. 446–455, 2006.

[13] T. Camilo, C. Carreto, J. Sá Silva, and F. Boavida, “An energy-efficient ant base routing algorithm for wireless sensor networks,” in Proceedings of the 5th International Workshop on Ant Colony Optimization and Swarm Intelligence (ANTS ’06), pp. 49–59, 2006.

[14] X. Jiang and B. Hong, “ACO based energy-balance routing algorithm for WSNs,” in Proceedings of the Advances in Swarm Intelligence (LNCS ’10), vol. 6145, pp. 298–305, 2010.
Submit your manuscripts at http://www.hindawi.com