Hindawi
Security and Communication Networks
Volume 2017, Article ID 7041381, 10 pages
https://doi.org/10.1155/2017/7041381

Research Article

BAS: The Biphase Authentication Scheme for Wireless Sensor Networks

Rabia Riaz,[1] Tae-Sun Chung,[2] Sanam Shahla Rizvi,[3] and Nazish Yaqub[1]

[1]*Department of CS & IT, University of Azad Jammu and Kashmir, Muzaffarabad 13100, Pakistan*
[2]*Department of Software, Ajou University, San 5, Woncheon-dong, Yeongtong-gu, Suwon 443-749, Republic of Korea*
[3]*Department of Computer Sciences, Preston University, 15 Shahrah-e-Faisal, Banglore Town, Karachi 75350, Pakistan*

Correspondence should be addressed to Sanam Shahla Rizvi; sanam_shahla@hotmail.com

Received 2 August 2017; Accepted 10 October 2017; Published 6 November 2017

Academic Editor: Huaizhi Li

The development of wireless sensor networks can be considered as the beginning of a new generation of applications. Authenticity of communicating entities is essential for the success of wireless sensor networks. Authentication in wireless sensor networks is always a challenging task due to broadcast nature of the transmission medium. Sensor nodes are usually resource constrained with respect to energy, memory, and computation and communication capabilities. It is not possible for each node to authenticate all incoming request messages, whether these request messages are from authorized or unauthorized nodes. Any malicious node can flood the network by sending messages repeatedly for creating denial of service attack, which will eventually bring down the whole network. In this paper, a lightweight authentication scheme named as Biphase Authentication Scheme (BAS) is presented for wireless sensor networks. This scheme provides initial small scale authentication for the request messages entering wireless sensor networks and resistance against denial of service attacks.

1. Introduction

A wireless sensor network (WSN) consists of a number of tiny devices called sensor nodes and a base station. These tiny devices may be few or thousands in number; it depends on the size of network. Sensor nodes can be easily deployed and the distance is normally less than few meters between two sensor nodes. Sensors can cooperate with each other to observe physical or environmental situations such as temperature, motion, and pressure. Nodes are used to detect, collect, and process environmental data. Due to small size, sensor nodes are resource constrained with respect to energy, memory, and computational and communicational capabilities [1, 2]. Nodes life period depends on their battery power. The base station is authoritative data processing and storage center and it is also called sink [3]. It usually serves as entryway to another network, is more dominant, and is resource enriched than sensor nodes. Any new node which wants to join the existing network, whether it is authentic user or not, is checked through base station [4].

There are two types of devices defined in IEEE 802.15.4 for WSN [5]. These devices are full-function devices (FFDs) and reduced-function devices (RFDs). RFDs have minimal resources and less memory capacity than FFDs. FFDs act as a personal area network (PAN) coordinator [6] but RFDs only work as worker node. FFDs can communicate with RFDs and all other FFDs in network, but RFDs can only communicate with near neighboring RFDs and FFDs.

WSNs are used in healthcare applications, military applications, environment and habitat monitoring, home automation, and traffic control. Due to their extensive usage in various domains, authenticity of communicating entities is vital for proper functionality of WSN. The purpose of authentication is to enable a sensor node to make sure of the identities of entities communicating with it. Authentication in WSNs is always a stimulating task due to the wireless nature of transmission media. The following two characteristics of WSNs make it challenging to provide an authentication mechanism for secure communication in WSNs.

(1) Resource Constraints. Sensor nodes have limited communicational and computational capabilities. Nodes have limited memory and energy availability. As sensor nodes are resource constrained [7–9], it is not possible for each node to authenticate all incoming request messages, whether these request messages are from authorized or unauthorized nodes. Any malicious node can easily send request message to join the network. All these resource constraints require that the authentication process should be efficient and lightweight for effective working of WSNs.

(2) Network Constraints. WSNs use wireless open channel. An invader can easily get access to the network and insert bogus messages in network. The network may transmit these fake request packets inserted by an invader many hops before they are identified by base station. Any malicious node can flood the network by sending fake request messages repeatedly to bring down the network by creating denial of service (DoS) attack. This results in consumption of network bandwidth and nodes energy, obstruction of communication among nodes, and disruption of the service to a specific system. As a result, it makes the system or service unavailable for the legitimate users. All these problems inversely affect the network lifetime and gradually reduce the functionality as well as the overall performance of the entire network. So there is requirement of some authentication mechanism, which can prevent the transmission of messages in the network, injected by an adversary, and provide partial authentication if not complete at initial message exchange time.

This research aims to exploit the problems of authentication in WSNs. In this study, an authentication scheme named as "Biphase Authentication Scheme" is proposed to make authentication process efficient and to overcome the authentication vulnerability in WSNs. The purpose of this scheme is to

(i) defend sensor network against DoS attack,

(ii) reduce network traffic,

(iii) save nodes battery powers,

(iv) increase the lifetime of WSN.

The functionality as well as the performance of the entire network improves by using the proposed scheme.

This paper is divided into following sections. Section 2 presents security requirements for WSNs, and some existing protocols, used for authentication process in WSNs, are reviewed with their advantages and limitations indicated. Section 3 provides an overview of the authentication process in WSNs. The main objective of this section is to introduce an authentication scheme named as Biphase Authentication Scheme (BAS) for WSNs. Section 4 highlights the network model used for performance evaluation. Section 5 provides the results obtained from the analysis of BAS by comparing it with previously proposed methods. Conclusion and recommendations for future work are presented in Sections 6 and 7, respectively.

2. Related Work

There are numerous schemes that provide authentication in WSNs [5, 10–17]; the most relevant of them are discussed in detail here.

2.1. Sensor Protocol for Information via Negotiation (SPIN). SPIN is a security scheme that provides authentication for WSN. It provides security but with great consumption of energy. SPIN has two main components, secure network encryption protocol (SNEP) and micro timed efficient stream loss-tolerant authentication (μTESLA) [10].

SPIN provides confidentiality, two-party data authentication, data integrity, and data freshness [11]. This protocol uses the trusted third party, which is central key distribution center (KDC), and overall communication between nodes takes place through it. In this scheme all key creation activities are performed through the base station. Its responsibility is to authenticate and create the session keys between nodes and send shared keys to communicating nodes. The KDC can communicate with nodes either directly or indirectly. In SPIN every node and the server share a unique key. Each node has an individual shared master key and this key is used for validation purpose of node by base station. All further keys are evaluated from the shared key.

This protocol depends on KDC for communication. Session keys are created and distributed through KDC. There is a lot of burden on base station in this scheme. Two nodes cannot directly establish a secret key with each other. If they wish to create secure communication session keys, they must first talk with the base station. In enormous scale network, the base station is many hops away. This feature is a drawback of this protocol; all the information passes through the base station. The traffic flow on sensor nodes nearby the base station is increased which results in consumption of energy [12].

In SPIN protocol, no proper solution is provided for information leakage or if a node is captured. The scalability of SPIN protocol is limited and it cannot easily applied to large scale sensor networks. It also suffers from denial of service (DoS) attack [13]. An adversary can easily send a request to the target node, and the target node forwards its request to KDC for authentication purpose. The adversary node can send network joining messages repeatedly to bring down the network by creating DoS attack, due to which the receiver node may lose its energy.

2.2. Broadcast Session Key Protocol (BROSK). BROSK is a broadcasting negotiation protocol which is used for secure communication in WSNs. In this protocol, no trusted party or server is used just like SPIN and it consumes less energy as compared to SPIN. Each node directly constructs a session key with its neighboring node by sending a key negotiation message [14]. This protocol uses a single master key in each sensor node for the entire WSN, and a message authentication code (MAC) is used to provide authentication. A sensor node will attempt to negotiate a shared session key by transmitting the key negotiation message. When node receives the message transmitted by its neighbor, it can establish the

mutual-session keys by creating the MAC and use these shared keys for secure message exchange.

The scalability of BROSK protocol is significant and it can easily apply to large scale sensor networks. In this protocol master key is not managed in a proper way and there is no proper information about master key, that is, what is done with the master key once the broadcasting process has completed. In BROSK protocol the same master key is shared by each node. This key is used by nodes to verify other nodes: whether node is authorized or unauthorized user. In this scheme no proper solution is provided for the problem if master key is compromised. An intruder can effortlessly compromise the whole network communication and create all further keys [15].

2.3. Localized Encryption and Authentication Protocol (LEAP). LEAP is used to provide security in sensor network [5]. In LEAP four types of keys are used which are individual keys, pairwise keys, cluster keys, and group keys. By using an individual key, a node can inform the base station about the anomalous behavior of its surrounding nodes. The base station uses this key to give instruction to a specific node. A master key is used to produce the individual keys and these keys are stored in nodes before their deployment.

Pairwise keys are shared by a node and its neighbors. These keys are used for secure communication. A node can establish pairwise keys by sending a message to the neighboring node. Cluster keys are shared by a node and its multiple neighbors. The node uses the pairwise key to encrypt the cluster key so that only the legitimate neighbors are able to decrypt the message to get access to the cluster key. A group key which is also called global key is shared by all nodes in the entire network. This key is used by the base station to encrypt data, and encrypted data is transferred to all the nodes in the group. This key removes the need for a base station to encrypt and send the same message to individual nodes with individual keys.

This protocol is effective in terms of communication and energy. It provides mechanisms for authentication broadcasting of a base station, data packets, and key revocation. The drawback of this protocol is security weakness during the process of key formation and the high cost of capacity needed to save the four keys for each node. In neighbor discovery phase of the pairwise key creation an invader can force a node to compute pairwise keys with many or all nodes. In this way any invader can easily compromise the node and get access to the pairwise keys without any information about the initial key.

2.4. A Dynamic User Authentication Scheme for Wireless Sensor Networks. A user authentication scheme for WSN prevents unauthorized users from querying the sensor data from any sensor node in network [16]. The computational overhead of this scheme is low. For authentication purpose, this scheme uses user's password and uses cryptographic hash functions. This scheme comprises three phases: registration, login, and authentication phase. This scheme permits only authentic users to query sensor data.

During registration phase, a user sends ID and a password for registration purpose to a gateway node. The gateway node stores the user ID and password in its database and tells the user about successful registration. When the user wants to query sensor data, it has to log in to a sensor login-node. The user sends its ID and password to the login-node. When the login-node receives the login request from the user, it checks the dataset list to find the user ID. If the ID is not found, then a rejection message is sent to the user. If the ID is found, then the login-node sends a message for authentication purpose to the gateway node. When the gateway node receives the message from the login-node, it checks its database to find the user ID. If the ID is not found, a rejection message is sent to the login-node. If the ID is found, then the gateway node sends an acceptance message to the login-node. The login-node then sends an acceptance message to the user.

This scheme has some flaws. It cannot provide resistance against replay and forged attacks. It also suffers from stolen-verifier attack; both gate way and login-node have the look-up table which contains secret information about registered users. Passwords may be exposed by any of the sensor nodes and the user is unable to alter the password.

2.5. An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks. It is a user authentication scheme [17] to overcome the flaws of user authentication scheme by [16] as it provides resistance against reply attack and forged attack, and it is a modified version of the user authentication scheme by [16]. In this scheme user can easily change password and can log in to the network from any sensor node and this scheme does not require additional computation.

This scheme comprises four phases which are registration, login, authentication, and password-changing phase. The registration, login, and authentication phases work in a similar way to the phases in the user authentication scheme by [16]. When a sensor node receives the login request from a user, it forwards this request to the gateway node. The gateway node confirms the legitimacy of the user. User registration is also performed at the gateway node. In password-changing phase, when a user wants to alter its password, it sends its ID, original hashed password, and new hashed password to the gateway node. When the gateway node receives the request for password change from the user, it checks the user ID and whether the hashed password sent by user is correct or not. If the ID is not found in its database or the hashed password is incorrect, then the gateway node sends a rejection message to the user. Otherwise, it changes the user password and sends the user a password change message. This scheme overcomes the flaws of the user authentication scheme by [16] but it also suffers from security flaws and is unable to provide resistance against node compromise attack.

3. Proposed Biphase Authentication Scheme (BAS)

Sensor nodes are usually resource constrained with respect to energy, memory, and computational and communication capabilities. It is not possible for each node to authenticate

Legend:
/: *Modulo 2 division operation*
$\mathfrak{I}$: *Truncates the input stream to 128 bits if* $r > 128$
KM: Master key of 1024 bits
S: Generator polynomial of 64 bits
R: Remainder after division between master key and seed
r: Number of bits in remainder
KE: 128 bits Encryption key
Begin Proc
$R = KM/S$
If $r\{R\} > 128$
$KE = \mathfrak{I}(R)$
Else
$KE = R$
End Proc

Algorithm 1: Key generation algorithm.

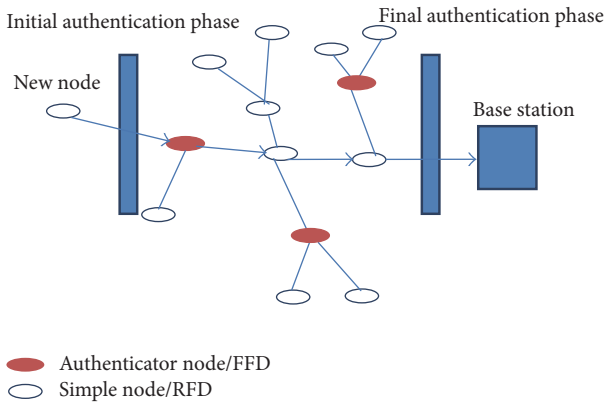

Figure 1: Authentication process using Biphase Authentication Scheme.

all the incoming messages. This scheme provides initial small scale authentication of the messages entering to WSNs.

There are two types of devices defined in IEEE 802.15.4 for WSN: full-function devices (FFDs) and reduced-function devices (RFDs). In this proposed scheme, FFDs will act as authenticator nodes. These authenticator nodes will forward the outside request messages to the base station as shown in Figure 1. In case of unauthorized node request message, these nodes will block the request message and will not forward it to the base station.

BAS comprises two phases: initial authentication phase and final authentication phase.

3.1. Initial Authentication Phase. The initial authentication phase is performed with the help of authenticator nodes. This phase acts as a filter, and authenticator nodes act as gateway nodes. Any new node that wants to join the network sends its request to the authenticator node. This phase blocks the request messages sent by an adversary in the network. Only authorized nodes request messages are sent to the base station for final authentication.

3.2. Final Authentication Phase. The final authentication phase is performed with the help of the base station. The base station matches the (ID, Key) pair sent by the authenticator node in its database. If they are matched, then the new node is successfully approved, and complete access to network will be permitted. An acceptance message will be sent to the new node through the authenticator node. If the (ID, Key) pair is not found, then the new node is not successfully approved, no access to network will be permitted, and a rejection message is sent to the authenticator node.

In BAS, each node is preloaded with *node ID, master key* K_M, *key generation algorithm,* and *pairwise shared key with base station* K_{NB} before their deployment. This scheme has been designed to be very lightweight and uses symmetric keys. Symmetric key system requires less storage than asymmetric key system, so this system is better than asymmetric key system for sensor networks [15]. Each node has its *unique ID, master key* K_M *of 1024 bits,* and *pairwise key* K_{NB} *of 128 bits* [18]. A base station has *[ID,* K_{NB}*]* pair for every node in its database and uses it to authenticate every sensor node at the time of node joining the network. K_{NB} is a unique pairwise key of each node with the base station. Base station can use this key to directly communicate with nodes.

In BAS, we use a modified form of key generation algorithm [19]. This algorithm is used to create the encryption key K_E from any random seed S of 64 bits. This random seed S is used for security purpose; when any authenticator node receives network joining request from any new node, it calculates the encryption key K_E from any random seed S by using key generation algorithm and sends the same random seed to new node. New node calculates its own encryption key K_E from random seed sent by authenticator node, then sends its calculated encryption key K_E to authenticator node, and authenticator node checks that encryption key calculated by new node is correct or not by comparing it with its own calculated K_E. This algorithm is depicted in Algorithm 1.

In BAS mechanism, initial authentication is performed between new node (A) and authenticator node (AN) and consists of the following steps if the node A is new node and it wants to join the network.

(1) The node A sends its ID to authenticator node.

$$M_1 = A \longrightarrow \text{AN} : [\text{ID}_A] \quad (1)$$

(2) Authenticator node receives message M_1 from A and performs the following functions.

(a) It calculates encryption key (K_E) using any random seed S and key generation algorithm; see Algorithm 1.

(b) It sends the same random seed to new node A.

$$M_2 = \text{AN} \longrightarrow A : [S] \quad (2)$$

(3) If node A is authorized user and it has master key K_M, it can easily obtain its own K_E by using the random seed S sent by the authenticator node and the key generation algorithm; see Algorithm 1.

(4) The node A sends K_E to authenticator node.

$$M_3 = A \longrightarrow \text{AN} : [K_E] \quad (3)$$

(5) Authenticator node receives M_3 from A and performs the following functions.

(a) It checks the K_E; if it is correct, it agrees to become its agent and an [In-Progress] message is sent to node A which means that node A is working on the authentication process.

$$M_4 = \text{AN} \longrightarrow A : [\text{In-Progress}] \quad (4)$$

(b) If K_E is incorrect, it refuses to become its agent and does not send new node request to base station.

(6) When node A receives message M_4 from authenticator node, it forwards its pairwise key K_{NB} to authenticator node.

$$M_5 = A \longrightarrow \text{AN} : [K_{NB}] \quad (5)$$

(7) Authenticator node forwards node A request to base station (BS).

$$M_6 = \text{AN} \longrightarrow \text{BS} : [\text{ID}_A, K_{NB}] \quad (6)$$

Final authentication is performed with the help of base station and consists of the following steps.

(8) BS receives message from authenticator node; it decrypts message, checks K_{NB} and ID_A sent by authenticator node by comparing them with values presented in its database, and performs the following functions.

(a) If they are matched, then new node is successfully approved and access to network is granted and [Accept] message is sent to authenticator node.

$$M_7 = \text{BS} \longrightarrow \text{AN} : [\text{Accept}] \quad (7)$$

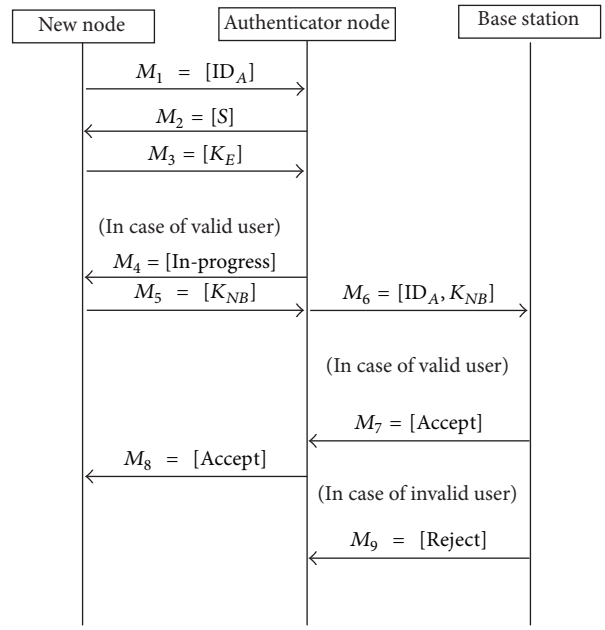

Figure 2: Working of Biphase Authentication Scheme.

(b) If they are not matched, then new node is not approved and no access to network is granted and [Reject] message is sent to authenticator node.

$$M_8 = \text{BS} \longrightarrow \text{AN} : [\text{Reject}] \quad (8)$$

(9) Authenticator node only sends [Accept] message to node A.

$$M_9 = \text{AN} \longrightarrow A : [\text{Accept}] \quad (9)$$

(10) On receiving [Reject] message authenticator node will not forward it to node A.

Complete authentication process of proposed scheme is summarized in Figure 2.

4. Network Model

We consider a WSN of 100 Mica2 sensor nodes and a base station. The network is arranged using the cluster-based topology [20]. Sensor nodes are arranged in cluster form, and every cluster has a node that acts as the cluster head (CH). In BAS network model, FFDs will act as CHs and all new nodes that want to join the network will forward their request messages to the CH. Each CH will send request to another nearby CH. Finally the request reached base station through multihop wireless communication via CHs.

The base station is also a Mica2 node with greater energy and computation capabilities. In cluster-based topology each node in cluster is one hop away from its CH. Each CH is one hope away from its neighboring CHs and many hops away from other CHs. Each CH forwards data to its closest CH. In our network model the farthest CH is at a distance

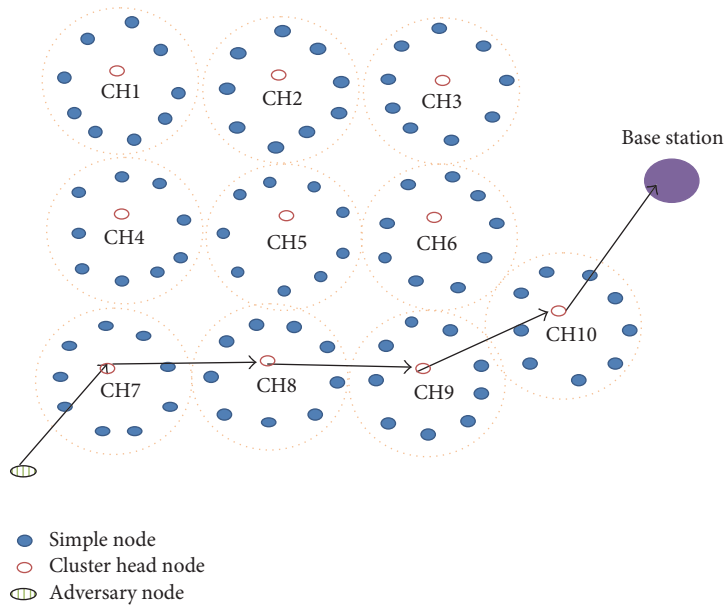

Figure 3: Cluster-based topology in SPIN.

of D hops from base station. For our scheme, we assume that $D = 4$. In BAS, CHs will also work as authenticator nodes. Mica2 nodes send and receive messages consuming 16.25 μJ/byte and 12.25 μJ/byte energy, respectively [21]. This energy consumption is for one hop distance and transmission energy consumption varies with respect to number of hops. Authenticator nodes/CHs consume 0.73 μJ energy [19] to obtain encryption key K_E by using key generation algorithm.

The following equations are used to calculate energy consumption of nodes in proposed network model.

(i) T_x is transmitting energy, R_x is receiving energy, and K_x is energy consumption to obtain encryption key.

(ii) E_{T_x} is total transmitted energy consumption of messages, which will be calculated as

$$E_{T_x} = (T_x * n) * H \tag{10}$$

Here n is the number of sent bytes by each CH and H is the number of hops used to send message to BS.

(iii) E_{R_x} is total received energy consumption of messages, which will be calculated as

$$E_{R_x} = (R_x * n) \tag{11}$$

Here n is the total number of received bytes in network.

(iv) E_{K_x} is the total energy consumption to obtain encryption key K_E, which is calculated as

$$E_{K_x} = (K_x * X) \tag{12}$$

Here X is the number of times encryption keys are generated by authenticator nodes in BAS.

(v) E_{Tot} is the total energy consumption, which will be calculated as

$$E_{\text{Tot}} = E_{T_x} + E_{R_x} + E_{K_x} \tag{13}$$

(vi) M_{Tot} is the total number of sent and received messages in the network, which will be calculated as

$$M_{\text{Tot}} = M_{S_x} + M_{R_x} \tag{14}$$

Here M_{S_x} is the number of sent messages and M_{R_x} is the number of received messages in the network.

5. Performance Evaluation

The performance of the proposed scheme BAS is evaluated for different metrics like energy consumption, packets ratio, and DoS attack. BAS was compared with one of the existing schemes, SPIN, by applying both schemes to the network model explained in Section 4.

5.1. Energy Consumption. When a new node wants to join the network, it has to send request to the base station and receive the reply message from it. The authentication of a node is checked at base station. This will result in consumption of nodes energy and an increase in network traffic. The basic purpose of BAS is to prevent the transmission of packets in the network injected by an adversary to enhance the life period of sensor network.

In SPIN protocol a new node which is an adversary sends request to CH, that is, CH_7 as shown in Figure 3. Then CH_7 forwards its request to nearby CH_8. Finally the request reached the base station after multihop wireless communication.

The total transmitted energy consumption is calculated by (10); see Section 4. In this case, four CHs are involved in

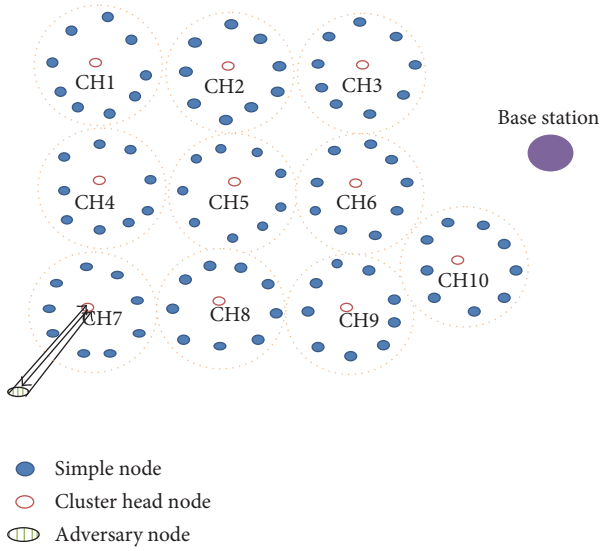

Figure 4: Cluster-based topology in BAS.

routing process (CH_7, CH_8, CH_9, and CH_{10}). The number of hops D is 4 as the farthest CH is four hops away from the base station. In SPIN protocol the length of message which consists of ID, symmetric key, and nonce bits is 36 bytes [22].

$$E_{T_x} = (16.25 * 36) * 4$$
$$E_{T_x} = 2{,}340\,\mu J \quad (15)$$

The total received energy consumption is calculated by (11). In the case shown in Figure 3, 36 bytes are received by each CH in network, so the total number of received bytes in network including the received bytes of base station is $n = 36 * 5 = 180$ bytes.

$$E_{R_x} = (12.25 * 180)$$
$$E_{R_x} = 2{,}205\,\mu J \quad (16)$$

The energy consumption to obtain encryption key in SPIN is zero as it is only used in BAS. The total energy consumption for SPIN is calculated by (13).

$$E_{\text{Tot}} = 2{,}340\,\mu J + 2{,}205\,\mu J = 4{,}545\,\mu J \quad (17)$$

In BAS new node A sends its ID to authenticator node. Authenticator node sends seed [S] to node A. The size of ID, seed, and encryption key K_E is 2, 8, and 16 bytes, respectively. Node A will send its own key K_E to authenticator node. Authenticator node checks new node's key; if it is incorrect, then it does not forward its request to base station. In this case, as shown in Figure 4, two messages are received by authenticator node and only one message is transmitted by it.

The total transmitted energy consumption in this case is calculated by (10).

$$E_{T_x} = (16.25 * 8) * 1 = 130\,\mu J \quad (18)$$

Table 1: Energy consumption comparison between SPIN and BAS.

Energy consumption $E_{\text{Tot}} = E_{T_x} + E_{R_x} + E_{K_x}$	SPIN	BAS
E_{T_x}	2,340 μJ	130 μJ
E_{R_x}	2,205 μJ	220.5 μJ
E_{K_x}	0	0.73 μJ
E_{Tot}	4,545 μJ	351.23 μJ

Here $H = 1$ as new node (adversary) is one hop away from the CH and the number of sent bytes of seed is $n = 8$ bytes.

The total received energy consumption is calculated by (11).

$$E_{R_x} = (12.25 * 18) = 220.5\,\mu J \quad (19)$$

Here the number of the received bytes is $n = 18$ bytes, including 2-byte ID and 16-byte encryption key.

The energy consumption in generating key K_E by authenticator node is calculated by (12).

$$E_{K_x} = 0.73\,\mu J * 1 = 0.73\,\mu J \quad (20)$$

Here $X = 1$, as only one key is generated by authenticator node.

The total energy consumption is calculated by (13).

$$E_{\text{Tot}} = 130\,\mu J + 220.5\,\mu J + 0.73\,\mu J = 351.23\,\mu J \quad (21)$$

An adversary can send request to some specific number of CHs to involve all CHs in the network. The total energy consumption will vary with respect to the number of CHs involved in routing process and with the total number of sent and received messages in the network. However, the energy consumption will be less in BAS compared to SPIN. Table 1 shows the energy consumption comparison between both schemes.

Simulation is used to evaluate the performance of proposed scheme. The results of this simulation are performed by using MATLAB. Figure 5 presents the energy consumption graph of BAS and SPIN scheme with respect to the number of adversary nodes. When the number of adversary nodes increases, the level of energy consumption also increases. This is because a higher number of CHs get involved in the routing process.

The results prove that energy consumption in proposed scheme BAS is much less as compared to SPIN scheme. So our scheme is helpful to improve the network performance and its lifetime by saving nodes battery power.

5.2. Packets Overhead. In SPIN protocol when an adversary sends a request to any node in the network, each node forwards the request to the base station. As a result, the traffic in the network near the base station increases, which reduces the performance of the whole network. In SPIN protocol when an adversary sends a request to CH_7 in the network, as shown in Figure 3, 4 packets will be sent and 5 packets will be received in the network.

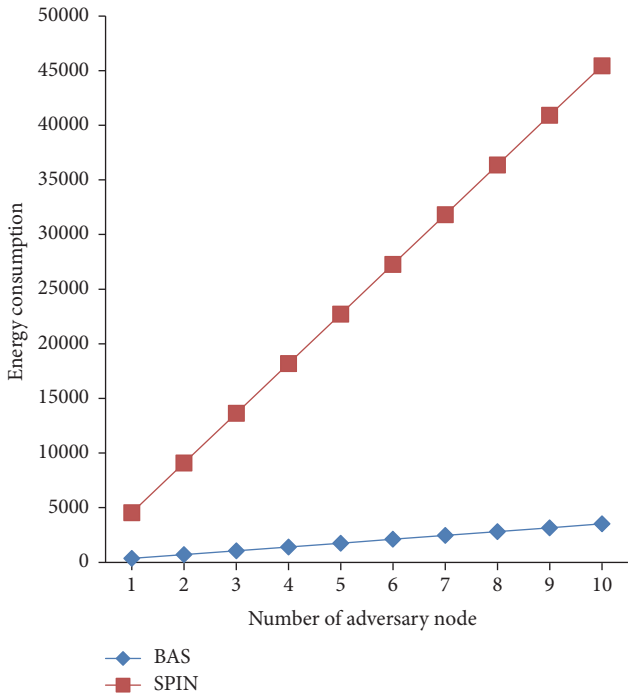

Figure 5: Variation of energy consumption with respect to number of adversary nodes.

Table 2: Packets overhead comparison between SPIN and BAS.

Total packets overhead $M_{\text{Tot}} = M_{S_x} + M_{R_x}$	SPIN	BAS
In case when an adversary sends request to CH_7	9	3

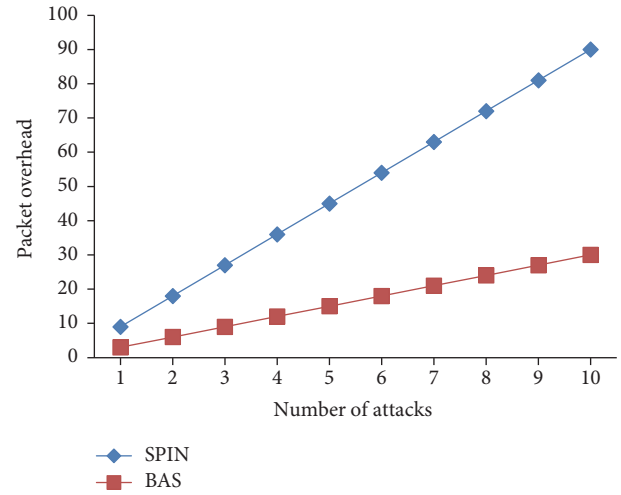

Figure 6: Variation of packets overhead with respect to the number of adversary nodes.

The total number of sent and received messages M_{Tot} is calculated by (14).

$$M_{\text{Tot}} = M_{S_x} + M_{R_x}$$
$$M_{\text{Tot}} = 4 + 5 \quad (22)$$
$$M_{\text{Tot}} = 9$$

In BAS only one packet will be transmitted by authenticator node and 2 packets will be received by it as shown in Figure 4.

The total number of sent and received messages M_{Tot} is calculated by (14).

$$M_{\text{Tot}} = M_{S_x} + M_{R_x}$$
$$M_{\text{Tot}} = 1 + 2 \quad (23)$$
$$M_{\text{Tot}} = 3$$

An adversary can send request to some specific number of CHs to involve all CHs in the network. The number of data packets will vary with respect to the number of CHs involved in routing process and the total number of sent and received packets in the network. However, the number of data packets will be less in BAS compared to SPIN scheme. Table 2 shows the data packets overhead comparison between both schemes.

We use simulation to evaluate the performance of the proposed scheme. Figure 6 presents the data packets overhead of BAS and SPIN scheme with respect to the number of adversary nodes. When the number of adversary nodes increases, the packets overhead in the network also increases. This is because a higher number of CHs get involved in the routing process, so the ratio of sent and received packets in the network is also high. However, the data packets overhead will vary with respect to the number of adversary nodes and the number of cluster heads involved in the routing process.

Results show that the total number of sent and received packets in the network will be less in BAS compared to SPIN scheme. So our scheme is helpful to improve the network performance and its lifetime by reducing network traffic.

5.3. Repeated Attacks (DoS Attack). DoS attack, also known as jamming attack, is main physical layer attack in WSN [23]. In this attack, an adversary repetitively send malicious requests in the network. Its purpose is to block availability of service to legitimate users, by creating DoS attack, by sending a number of messages continuously in the network.

In SPIN protocol when an adversary sends request to any CH or a number of CHs in the network, the whole authentication process will be performed to check authenticity of adversary node. Any malicious node or a number of malicious nodes can send the request messages repeatedly after short intervals of time, due to which all the CHs will be involved in the routing process and will gradually lose their battery powers. DoS attack will occur in the network, which will make the system or service unavailable for the authorized users.

In BAS when an adversary sends request to any CH in the network, only one packet will be transmitted by CH and 2 packets will be received by it. Similarly even if the same

adversary node sends request to some specific number of CHs or to all CHs in the network, only one packet will be transmitted and 2 packets will be received by every CH. There is no risk of DoS attack in the network and no disruption to the availability of the service to authorized users.

So the proposed BAS scheme is helpful to defend WSN against DoS attacks and improve the functionality and performance of the entire network.

6. Conclusion

The proposed Biphase Authentication Scheme (BAS) improves the performance and increases the lifetime of network. The main objective is to provide outside authentication for the user that wants to join the existing WSN. By using the proposed scheme, request messages of nodes can be filtered and messages of only partially authorized users are sent to the base station for final authentication. Initial authentication phase reduces the network traffic, and through final authentication phase only authorized nodes are able to become a part of the network. This scheme is helpful to overcome the flaws in existing schemes, that is, SPIN and BROSK.

It provides the solution for issues in SPIN scheme. SPIN protocol suffers from DoS attack, energy consumption, and network traffic problem. BAS overcomes these issues as shown in Section 5, so this scheme is better than SPIN scheme and improves the performance of the network.

In BROSK protocol the same master key is shared by each node. All other keys for communication are created from the master key. If the master key is compromised, then an invader can easily compromise the whole network and create all further keys.

BAS provides a solution for this problem. If the master key is compromised, an adversary cannot compromise the entire network and cannot produce further keys for communication. So this scheme provides more secure environment for network functionality than BROSK protocol and removes security vulnerabilities.

7. Future Work

WSNs are exposed to security attacks due to wireless nature of the media. Current authentication schemes used for WSNs cannot provide satisfactory solution for authentication vulnerabilities in network. There are other problems such as data integrity and confidentiality in WSNs. Further authentication schemes should be developed to provide outside as well as inside network security in WSN. Several extensions of this research work can be further developed. For future work our plan is to extend the proposed Biphase Authentication Scheme to provide inside network security such as data integrity, data freshness, and data confidentiality. This will overcome inside network authentication vulnerabilities in WSN like authentication vulnerabilities in network, will provide more secure environment for proper functionality of WSNs, and would be very effective to increase network performance. The effect of various nondeterministic factors, such as distance between nodes, remaining energy level of CH, and so forth, on BAS will also be carried out.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This research was supported by the Ministry of Science and ICT (MSIP) under ICT R&D program (2017-0-01672) supervised by the Institute for Information & Communications Technology Promotion (IITP).

References

[1] S. S. Rizvi and T.-S. Chung, "PIYAS-Proceeding to intelligent service oriented memory allocation for flash based data centric sensor devices in wireless sensor networks," *Sensors*, vol. 10, no. 1, pp. 292–312, 2010.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[3] S. S. Rizvi and T. S. Chung, "Performance evaluation of indices-based query optimization from flash-based data centric sensor devices in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 258080, 10 pages, 2012.

[4] R. Riaz, S. S. Rizvi, E. Mushtaq et al., "OSAP: online smartphone's user authentication protocol," *International Journal of Computer Science and Network Security*, vol. 17, no. 3, pp. 7–12, 2017.

[5] J. Zheng and M. J. Lee, "Will IEEE 802.15.4 make ubiquitous networking a reality?: a discussion on a potential low power, low bit rate standard," *IEEE Communications Magazine*, vol. 42, no. 6, pp. 140–146, 2004.

[6] A. Koubaa, M. Alves, and E. Tovar, "IEEE 802.15.4 for wireless sensor networks: a technical overview," in *Proceedings of the 11th IEEE International Conference*, pp. 400–406, 2005.

[7] M. Hoberl, I. Haider, and B. Rinner, "Towards a Secure Key Generation and Storage Framework on Resource-Constrained Sensor Nodes," in *Proceedings of the International Conference on Embedded Wireless Systems and Networks*, pp. 313–318, 2016.

[8] S. Prasad, S. Jaiswal, N. S. V. Shet, and P. Sarwesh, "Energy aware routing protocol for resource constrained wireless sensor networks," in *Proceedings of the 1st International Conference on Informatics and Analytics, ICIA 2016*, August 2016.

[9] D. Granlund, P. Holmlund, and C. Åhlund, "Opportunistic mobility support for resource constrained sensor devices in smart cities," *Sensors*, vol. 15, no. 3, pp. 5112–5135, 2015.

[10] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113–127, May 2003.

[11] B. Lai, S. Kim, and I. Verbauwhede, "Scalable session key construction protocol for wireless sensor network," in *Proceedings of IEEE Workshop on Large Scale Real Time and Embedded Systems (LARTES)*, pp. 1–6, 2006.

[12] S. S. Rizvi and T.-S. Chung, "Investigation of in-network data mining approach for energy efficient data centric wireless sensor networks," *International Review on Computers and Software*, vol. 8, no. 2, pp. 443–447, 2013.

[13] J. Gul, S. Mushtaq, and R. Riaz, "Optimal guard node placement using SGLD and energy factor," *Journal of Computing*, vol. 4, no. 6, pp. 87–92, 2012.

[14] B.-C. C. Lai, S. P. Kim, I. Verbauwhede, and D. D. Hwang, "Reducing Radio Energy Consumption of Key Management Protocols for Wireless Sensor Networks," in *Proceedings of the 2004 International Symposium on Low Power Electronics and Design, ISLPED 2004*, pp. 351–356, August 2004.

[15] K. Kifayat, M. Merabti, Q. Shi, and L. J. David, "Security in wireless sensor networks," in *Handbook of Information and Communication Security, 2010, Part E*, pp. 513–552, 2010.

[16] K. H. M. Wong, Y. Zheng, J. Cao, and Wang, "A dynamic user authentication scheme for wireless sensor networks," in *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, pp. 318–327, 2006.

[17] H. R. Tseng, R. H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in *Proceedings of the 50th Annual IEEE Global Telecommunications Conference (GLOBECOM '07)*, pp. 986–990, November 2007.

[18] R. Riaz, *A Unified Security Framework for IP Based Wireless Sensor Networks [Ph.D. thesis]*, 2008.

[19] R. Riaz, A. Naureen, A. Akram, A. H. Akbar, K. H. Kim, and H. Farooq Ahmed, "A unified security framework with three key management schemes for wireless sensor networks," *Computer Communications*, vol. 31, no. 18, pp. 4269–4280, 2008.

[20] Q. Mamun, "A qualitative comparison of different logical topologies for wireless sensor networks," *Sensors*, vol. 12, no. 11, pp. 14887–14913, 2012.

[21] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for networked sensors," in *In Proceedings of the ACM ASPLOS IX*, pp. 93–104, 2000.

[22] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, pp. 2–22, 2006.

[23] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.