Computers and Electrical Engineering 48 (2015) 405–416

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Reliable anonymous secure packet forwarding scheme for wireless sensor networks ☆

S.V. Annlin Jeba [a,*], R. Suresh Kumar [b]

[a] Department of Computer Science & Engineering, C.S.I. Institute of Technology, Tamil Nadu, India
[b] Department of Mathematics, C.S.I. Institute of Technology, Tamil Nadu, India

ARTICLE INFO

Article history:
Received 19 July 2014
Received in revised form 26 August 2015
Accepted 28 August 2015

Keywords:
Anonymity
Identity
Optimal route
Communication
Link quality
Security

ABSTRACT

Designing a lightweight, secure communication protocol for Wireless Sensor Networks (WSNs) remains a challenging issue since sensor networks are resource limited and are left unattended. Sensor nodes in WSNs are subjected to varying forms of attacks. An adversary may destroy or damage the communications done in multi-hop WSNs by means of packet dropping and modification. Hence it is essential to have an efficient cryptographic scheme to protect the communications done in WSNs. This study introduces a Reliable Anonymous Secure Packet forwarding (RASP) scheme that can prevent not only traffic analysis attack but also the attacks done through compromised forwarding nodes. The mechanisms followed here are effective with low computation and communication overhead. The performance of the proposed scheme is evaluated over NS2 with a series of simulation. The simulated results show that the proposed scheme performs better than other comparable schemes.

1. Introduction

Rapidly developed WSN technology is widely used in different types of applications due to its economic and viable nature. A WSN is composed of a large number of sensor nodes which are connected through wireless links. The sensor nodes send data to Base Station (BS) through multi-hop transmission. The Wireless nature of communication, resource limitation on sensor nodes and unknown network topology prior to deployment makes the sensor nodes vulnerable to various security attacks [1,2]. From the security standpoint it is essential to provide authentic and accurate data to the BS. Previous security schemes focus on security services such as authenticity, confidentiality and integrity [3]. In addition to these services, many applications of WSNs have special requirements in terms of privacy and security [4,5].

Different key management schemes [6–8] have been developed to ensure data security in different circumstances for WSNs. Security relevant issues in WSNs and the issue of key establishment are considered in this literature [6]. Key predistribution through public key cryptography has been demonstrated in [7]. Energy limitation of sensor nodes make the use of public key systems impractical for WSNs. Security in hierarchical WSNs can be achieved using combinatorial designs [8,9]. This scheme assigns key chains to sensor nodes before deployment which reduces communication overhead. However, it requires more key space and it is not an energy efficient mechanism. To overcome these issues full pairwise key management

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. M.H. Rehmani.

* Corresponding author.
E-mail addresses: annlin_jeba@yahoo.co.in (S.V. Annlin Jeba), sureshannlin@gmail.com (R. Suresh Kumar).

http://dx.doi.org/10.1016/j.compeleceng.2015.08.021
0045-7906/

scheme can be adopted [10]. This is achieved by sharing pairwise key between neighbouring nodes. In a WSN with '*n*' nodes each node desires its key to be predistributed with $n-1$ nodes [11]. This scheme causes storage of large number of keys in each node. Moreover, maintaining forward and backward secrecy through this scheme is also a challenging task. If a node is compromised all the secure links connecting the compromised node with other nodes get affected. To reduce the node compromisation probability random key predistribution scheme can be followed. In random key predistribution process each node is assigned with a ring of keys selected randomly from a key pool [11]. But when a node is compromised all its keys and all the links secured by these keys are also compromised.

Recently many approaches have been proposed for providing hop-by-hop authentication [12]. These mechanisms need to share pairwise key between consecutive neighbouring nodes along with the selected path. But these schemes may function efficiently if all the links in the network are highly resilient to compromisation. [13].The proposed RASP mechanism considers security and privacy as important concern in packet forwarding. Further, it avoids unauthorised and infected traffic from being forwarded to the next hop. Simulation results and analytical studies verify the achievability of the proposed scheme.

1.1. Contributions

The key contributions of the proposed scheme are as follows:

- This scheme ensures reliability in communication by selecting optimal forwarding nodes which avoids frequent failure of nodes along with the selected path.
- It preserves the privacy of the sensor nodes involved in communication through the security service anonymity. This feature prevents the occurrence of traffic analysis attack.
- Incremental hash based authentication technique is followed in this scheme which allows immediate authentication of the packets received. This mechanism prevents compromised data from being forwarded in the network.

1.2. Notation

For the reason of clarity, the notations used throughout this study are listed in Table1.

The rest part of the paper is organised as follows. Some literatures related to the proposed scheme are discussed in Section 2. Section 3 presents the detailed description of the proposed scheme, followed by analysis and discussion in Section 4. Analysis through simulation is presented in section 5. The proposed mechanism is concluded in Section 6.

2. Related works

Recently, many secure communication schemes have been investigated by researchers to resist the vulnerabilities caused in WSNs. Some of the related schemes and their security relevant issues have been presented in this section. Literature

Table 1
Notations.

Notations	Descriptions
S_{ID}	Source identity
H()	Hash function
Enc $_{SID}$	Encryption using source identity
Pkt_info	Encrypted message in the packet
Auth_info	Authentication information
REQ	Format of request message
BS_{ID}	Base station identity
Hop_{ID}	Identity of the next hop or forwarding node
XOR	Exclusive OR
Dec_{SID}	Decryption using S_{ID}
REP	Format of the reply message
SK	Secret key
SD	Secured data
RS	Random string
Enc $_{SK}$	Encryption using secret key
t_w	Time window
RE_{thres}	Threshold value for residual energy
T_{source}	Time consumed by source to generate report
T_{hop}	Time consumed by forwarding node
T_{BS}	Time consumed by base station
T_{Hash}	Time to perform single hash operation
T_{XOR}	Time to perform single exclusive OR operation
T_{Rand}	Time for random selection of 128 bits
T_{Dec}	Time to decrypt a message
T_{Enc}	Time to encrypt a message
||	Concatenation operator

includes concepts regarding end-to-end security mechanisms; hop-by-hop authentication schemes and identity based cryptographic techniques.

Kalyani and Chellappan [7] proposed RSA-CRT an asymmetric key management scheme. This scheme improves the performance of RSA algorithm and provides countermeasures for attacks performed in network layer. Moreover, authenticated message broadcast can also be achieved through this scheme. But this scheme involves high energy consumption due to its complicated computation. Oliveira et al. [14] discussed about a secure communication scheme, SecLEACH to ensure security in hierarchical WSNs. The random key predistribution mechanism followed here increases the secrecy of the data in transit. This scheme suffers from orphan node problem since the key ring assigned for a node is not sufficient to share pairwise symmetric keys with all the nodes in a WSN.

Lu et al. [15] presented an effective key management scheme for cluster-based WSNs. The author suggested two Secure and Efficient data Transmission (SET) mechanisms, identity-Based digital signature SET-IBS and identity-Based Online/Offline digital signature (SET-IBOOS). The basic idea enforced in these mechanisms is to encrypt and authenticate the sensed data using node ID and the private key shared with the BS. This scheme solves the orphan node problem through identity based cryptographic (IBC) operations. This scheme achieves confidentiality through asymmetric key management and it requires a digital signature for authentication. In addition, it is necessary to preload each sensor node with large number of system parameters. This leads to leakage of user's public key and secret key through compromised users.

Yu et al. [16] developed a mechanism for achieving end-to-end secure communication between sensor nodes in WSNs and internet users. The author uses two models to connect WSNs to internet. In the first model, BS is used as an interface between internet users and the sensor nodes. When an encrypted data is received by the BS, it decrypts the information received before directing the message towards the specified destination. This model reduces the scalability and increases computation complexity since the decryption and re-encryption operations are performed by BS. Further, all the traffic appears to be visible for the BS. Wen [17] presented an ID based remote user authentication scheme. This scheme achieves key revocation and off-line password change through identity based cryptographic operations. Hence, this scheme is highly resilient to impersonation attack.

Several studies including SEF [18], DEF [19] achieves link level security through hop-by-hop authentication. Also these schemes require encryption and decryption processes to be done at the intermediate nodes. Besides, these schemes require an association to be maintained between upstream and downstream neighbouring nodes. If a link is compromised then the communications performed through compromised links can be detected through uncompromised downstream forwarding nodes and dropped. Ren et al. [20] proposed a location aware end-to-end secure communication (LED) scheme. Different number of symmetric secret keys is assigned with each sensor node to provide end-to-end confidentiality and node-to-node authentication. LED avoids keys sharing but the keys assigned to a node are static and binded with location information. If a node belonging to a cell is compromised, then the chance for compromising the neighbouring node of the same cell is high.

Gu et al. [21] proposed a methodology called differentiated key predistribution. The core idea is to divide the sensor nodes into classes and to predistribute different number of keys to different sensor nodes. This scheme is highly resilient to fake packet injection and selective forwarding attack. But the computations performed to distribute the keys are complex and require more key space for storage.

Park and Jung [22] proposed a mechanism to provide anonymity in WSNs. Privacy is achieved in this scheme through phantom ID and SMAC. The phantom IDs are generated by means of a Hidden Vector (HV) and a timestamp value. This scheme is computationally expensive and cause additional delay in transmission. So it is necessary to use a solution with some kind of pseudonyms. Sho [23] proposed a mechanism to represent source anonymity. This scheme examines the issues against statistical source anonymity. Through analysis the author determined that the proposed mechanism causes high latency in reporting the real event information.

Lu et al. [24] described a Bandwidth Efficient Co-operative Authentication (BECAN) Scheme for detecting false data injected by compromised forwarding nodes. This scheme uses a bit compressed authentication mechanism to identify inaccurate data. For authentication purpose each forwarding node collects MAC (Message Authentication Code) from 'K' neighbours and generate a final MAC through CNR (Co-operative Neighbour Router) based authentication mechanism. This scheme ensures security by providing link level authentication. But the downside of this scheme is the computation complexity in generating MACs for 'K' neighbours and compressing into a single bit. The proposed RASP improves related works in several ways. Different from the above works, RASP does not require complicated security association between neighbouring nodes and maintains long-lasting relationship between en-routing nodes.

3. Proposed scheme

This section describes in detail about a secure communication framework designed for WSNs. The system under consideration consists of a static WSN with one node acting as a BS. Before initiating communication, the system parameters are predistributed to sensor nodes. When a source node is triggered by an event, it generates an event report and forwards the report towards the BS. The source node needs to determine a reliable path for forwarding the report. Each forwarding node verifies the authenticity of the report in transit. The various operations performed for protecting the communications done in the network are divided into four phases: Next hop selection, secure session setup, key generation and dissemination, anonymous packet transmission.

3.1. Description of the proposed scheme

This section provides a detailed description of the procedures followed in each phase.

3.1.1. Next hop selection

When a sensor node has sensed event information to be reported to the BS, it invokes the route discovery procedure to determine the forwarding node. This scheme determines the route based on the decision of intermediate nodes. In the proposed routing approach the forwarding nodes are decided based on their link status and their residual energy level. Initially, source node broadcasts a 'Hello' message. The 'Hello' message permits the node to learn information about its one hop and two hop neighbours. In addition, the source node maintains two different lists and updates the lists based on the reply received. One list (list1) holds data about its one hop neighbours and the other list (list2) preserves information about the minimum number of one hop neighbours that cover all its two hop neighbours. The procedure followed for determining a path between source and destination is given in Algorithm 1.

After collecting the information about its one hop and two hop neighbours, source broadcast route request message to all the members of list2 as stated in line 4. The nearby nodes receiving the route request message may reply with ⟨neighbour information, Link Quality (LQ), Residual Energy (RE)⟩ as represented in line 5. Based on the reply message, neighbour node with high LQ value and RE greater than the threshold (RE_{th}) will be selected as a suitable forwarding node. The selected node further broadcasts the route request message to identify suitable forwarder list. The same process gets repeated until a forwarding node finds its next hop as the BS. The proposed routing scheme updates list1 and list2 periodically to maintain route refreshness. Thus by using the proposed routing scheme a reliable route is established between the source and the BS.

Algorithm 1. Reliable path determination

Input: Link Quality, Residual Energy
1: Source node broadcast Hello packet containing source details
2: Node receiving the Hello packets responds with neighbour information
3: Source node generates and maintains two lists
  3.1: List1 = {one hop neighbours}
  3.2: List2 = {one hop neighbours that cover all two hop neighbours}
4: Source node send route request message to members of list2
5: Members of list2 send reply message including node ID, Link Quality, Residual Energy
  5.1: Each node Compute Link Quality periodically
    Link quality = $\frac{\text{packets successfully received in } t_w}{\text{Total packets transmitted in } t_w}$
6: Source node selects a node with maximum LQ value and RE > RE_{thres}
7: The selected node repeats steps 1 to 6 to select its next hop
8: Repeat steps 1 to 6 until a node find its next hop as the BS

3.1.2. Secure session setup

In this phase the source node initiate a secure request response session and provide security states for the forwarding nodes of the session. The operations performed by the forwarding nodes are represented in Algorithm 2. The source node generates an authenticated request message including source identity (ID), destination ID, a random string in encrypted format, authentication information and session ID as represented in line 6 of Algorithm 2. Source node forwards the request message to its next hop. The forwarding node receiving the request message authenticates the source node by verifying Auth_info contained in the message. If found authenticated, then updates the auth_info as represented in line 14. Further, forwards the updated message to the next hop. When the next hop receives the request message, it first authenticates its upstream forwarding node with the help of the Auth_info contained in the message. If found authenticated, then compute the Auth_info associated with the current forwarding node and update the request message with new Auth_info as represented in lines 11 to 15.

If the message is found to be illegitimate, the packet is dropped and the unauthorised upstream forwarding node is identified as the compromised node. The same process gets repeated until a forwarding node finds its next hop as the BS. The BS after receiving the request message verifies the authenticity of the packet. If the packet is found to be authentic, then it retrieves the Random String (RS) stored in encrypted form. Afterwards the BS records the retrieved 'RS' and associates it with the source node. The recovered 'RS' functions as a random challenge shared between the source and BS which ensures security for future communication. Updating authentic information at every hop increases the strength of authentication information endorsed in the packet. In addition, this scheme guarantees the privacy of the authentication information in transit.

Algorithm 2. Authenticated request forwarding (forwarding node, Destination node)

Input: Authenticated request message REQ
1: Source computes $S_{ID}^1 = H(S_{ID})$
2: Generates random string RS
3: pkt_info = Enc $_{SID}$ (S_{ID}, RS)
4: Auth_info = (pkt_info) XOR (S_{ID}^1)
5: Session information Se = H (session ID)
6: REQ = S_{ID}^1, BS_{ID}^1, pkt_info, Auth_info , Se
7: Source forwards the packet containing REQ message
8: For each hop along the selected path
9: If (Hop_{ID} != BS_{ID}) then
10: Next_hop computes Auth_info and Se
11: Check whether computed values matches with the received values
12: If matches then
13: Update Auth_info and Se of the REQ message
14: Updated Auth_info = H (Hop_{ID}) XOR (pkt_info)
15: Updated Se = H (Se)
16: else
17: Drop the packet
18: else if (Hop_{ID} = BS_{ID}) then
19: Verify and validate the Auth_info of the received REQ message
20: Retrieve RS from the encrypted pkt_info of REQ message
21: Store received RS and associates it with the source node
22:End

3.1.3. Key generation and dissemination

This phase describes the operations carried out by the BS and the forwarders in generating and distributing the key to the intended source node. The procedure followed for key generation and sharing process is presented through Algorithm 3. In

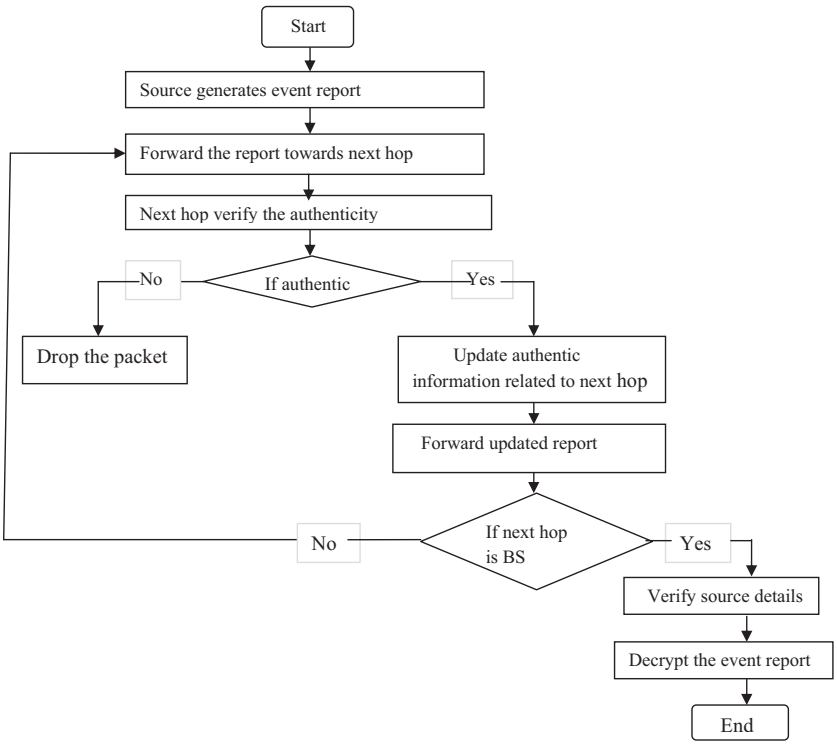

Fig. 1. Flow diagram for procedure of secure data transmission.

this phase a symmetric secret key is generated by the BS and it is shared with the source node without auxiliary message exchange. Initially the BS computes an Initialisation Vector (IV) by concatenating the RS received from the source node with the identity of the source node (S_{ID}). The computed IV is given as an input to a cryptographic hash function, SHA-2 algorithm. The hash function provides a message digest of 512 bits. The Genkey function selects 128 bits randomly from the message digest (512 bits) to function as a Secret Key (SK). To carry out secure data transmission, the SK used for encryption should be shared with the source node in protected form. The SK is protected by performing exclusive-OR operation with the random string already shared by the source node. The protected secret key is securely transmitted to the source node by means of an authenticated reply message. BS forwards the reply message towards the source node. The upstream forwarding node receiving the reply message verifies the authenticity of the message. This is done by computing authentication information (Auth_info) for the received packet and comparing with the Auth_info in the received packet. If both the values matches, then update the reply message with new Auth_info associated with current forwarding node. Subsequently forward it towards the source node. When the source node receives the reply message, it decrypts the packet information and retrieves the SK by doing excusive-OR operation of SD with RS. Thus the symmetric secret key is securely shared between BS and the source node. The SK value is refreshed for every session to increase the security strength of the data communicated.

Algorithm 3. One time secret sharing

Input: Random String
Reply message
1: BS generates an Initialisation Vector (IV)
2: IV = $(RS||S_{ID})$
3: BS performs cryptographic hash operation over IV
4: Hashed Value (HV) = H (IV)
5: SK = Genkey (HV)
6: BS protects the SK by creating Secured Data (SD)
7: SD = RS $\oplus$ SK
8: BS sends the REP message holding secured SK towards the source node
9: REP = S^1_{ID}, BS^1_{ID}, pkt_info, Auth_info , Se
10 : Pkt_info = Enc $_{SID}$ (S_{ID}, SD)
11: Auth_info = (pkt_info) XOR (BS^1_{ID})
12: Se = H (session ID)
13: Next_hop receiving the REP message verify the Auth_info enclosed in the message
14: If Auth_info is found to be valid then
15: Update Auth_info and Se of the REP message
16: Updated Auth_info = H (Hop_{ID}) XOR (pkt_info)
17: Updated Se = H (Se)
18: else
19: Drop the packet
20: If (Next_hop = source node) then
21: Source node receives REP message
22: Get the encrypted pkt_info
23: Retrieve SK: = RS $\oplus$ SD
24: End

3.1.4. Anonymous packet transmission

When an event is sensed by a sensor node, it needs to report the event information to the trusted entity, the BS. Due to vulnerabilities performed in wireless communication, it is essential for the sensor node to report the event information in protected form. The proposed scheme focuses on generating secured and authenticated event report using the security credentials shared by the BS. Also this scheme preserves the privacy of the information in transit by hiding the source and destination details. The detailed description of the operations performed in secure communication phase is as follows.

The event report generated by the source node consists of four fields. First field specifies the details about the source node. Destination node details are represented in the second field. Authentication information is placed in the third field. Further, the data along with the integrity value is specified in the fourth field. The format for the event report is specified as follows

$$\{[H(S_{ID})] : H(BS_{ID}) : (H(S_{ID})XOR(H(Enc_{SID}(Enc_{SK}(data)))||H(data))) : ((Enc_{SID}(Enc_{SK}(data)))||H(data))\}$$

Let the event information in the transmitted packet specified in the fourth field be represented as

$$pkt = ((Enc_{SID}(Enc_{SK}(data)))||H(data))$$

Hence the format of the packet in transit can be represented as

$$\{[H(S_{ID})] : H(BS_{ID}) : (H(S_{ID})XOR\ H(pkt)) : pkt\}$$

The next hop (Hop1) receiving the report check for authentication by means of the value maintained in the last field and the ID of upstream forwarding node. If the received packet is found to be authentic, then check whether it is the destination node. If this is not the destination node, then update the authentication information and forward the event report along the selected path. The format of the updated packet is given by

$$\{[H(S_{ID}) : H(BS_{ID}) : ((H(Hop1_{ID})XOR\ H(pkt)) : pkt\}$$

The authentication and report updating operation has to be performed by all intermediate hops along the selected path. When the event report is received by the BS, it verifies the authenticity of the received packet. If found authentic, then it retrieves the source detail of the packet received. Once determined, the BS decrypts the protected event data using the secret key shared with the source node. Then it performs integrity check to ensure correctness of the data received. Thus secured data transmission is performed through the proposed scheme.

The proposed scheme is able to achieve anonymous secure data transmission. This scheme prevents the exposure of entities involved in communication by hiding source ID and destination ID. Even by compromising an en-route node an adversary is unable to recover information regarding secret key or session key used for ensuring security. The flow diagram representing the sequence of operations performed for achieving secure communication is shown in Fig. 1.

4. Analysis and discussion

This section analyses the complexity of the proposed scheme in terms of computational requirements and the communications done in providing security for the sensed event information. Moreover, the security of the proposed scheme against the possible attacks has been analysed.

4.1. Complexity analysis

Complexity of the proposed scheme can be evaluated by the computational requirements and the communications performed in each phase of the proposed scheme. The computational complexity can be assessed by determining the number of operations and computations done in different phases for providing security requirements for the data packet to be transmitted. The communication cost is computed by determining the number of messages exchanged between the sensor nodes and the size of the messages communicated for achieving reliable route, establishing secure channel, ensuring secrecy in key sharing and data sharing.

4.1.1. Computational requirement

In the proposed routing mechanism only minimum number of operations is performed to compute the routing criterion such as link quality and residual energy of the sensor nodes. Likewise, in secure session setup phase one exclusive-OR operation, one encryption operation and three hash operations are performed in generating the authentication message. Besides, one hash and one exclusive-OR operation are performed in verifying the authentication message. The computational complexity of the key generation and dissemination phase is determined by the total time consumption for various operations performed in key generation and sharing. Time consumed by different nodes involved in key generation and distribution is given by the following equations.

$$T_{source} = 3T_{Hash} + T_{XOR} + T_{Enc} \tag{1}$$

$$T_{hop} = 2n(2T_{Hash} + T_{XOR}) \tag{2}$$

$$T_{BS} = 4T_{Hash} + T_{XOR} + T_{Dec} + T_{Rand} + T_{Enc} \tag{3}$$

where, n – number of forwarding nodes

4.1.2. Communicational requirement

The communications performed in determining reliable route includes transmission of two request messages and receiving two reply messages between the communicating entities. One message for collecting neighbour details and the other request for collecting routing parameters. In secure session setup phase single authentication message is transmitted between any two consecutive nodes. The Size of the message packet on transmission is equal to $|H(S_{ID}) + |H(BS_{ID}) + |H(Auth\_info)| + |H(pkt\_info)|$. The length of node ID is 2 bytes, length of authentication message is 20 bytes and length of data is 20 bytes. Hence the size of packet on transmit is 44 bytes. In key distribution process the secret key is securely shared through a single to and fro communication done between source and destination. Further, in anonymous packet transmission phase security in data transmission is achieved without auxiliary message exchange.

4.2. Security analysis

In order to evaluate the security of the proposed scheme, it is necessary to determine the vulnerabilities and the attacks that threaten the techniques followed in the proposed mechanisms. This section explains about the attacks and the countermeasures achieved through the proposed mechanisms.

4.2.1. Attack models

The possible attacks that may affect the security services of the proposed scheme can be passive attacks on transit, active attacks on transit, node compromisation attack and traffic analysis attack.

Passive attack on transit: Passive attackers are able to eavesdrop the packet at any point along with the communication path.

Active attack on transit: Active attackers can perform great damage to the packet on transit.

Node compromisation attack: In this category of attack an attacker can compromise a sensor node and retrieve all the secret credentials maintained by the compromised nodes.

Traffic analysis attack: An adversary may collect the traffic details continuously for a period of time and perform traffic analysis attack to know about the source and destination nodes involved in communication.

4.2.2. Countermeasures to the attacks

4.2.2.1. Resilient to passive attacks during communication. The event report communicated contains the security features confidentiality, authentication, integrity and anonymity. The adversary is able to retrieve the secured event report through eavesdropping. But he cannot retrieve the secret information contained in the event report. Further, the adversary is unable to obtain the source and destination details specified in the event report. Hence, it is determined that the proposed secure communication scheme has the solutions to function as countermeasure for passive attack.

4.2.2.2. Resist certain active attack on the path of communication. The proposed scheme is resilient to some of the active attacks such as selective forwarding and forwarding a falsified report. In the proposed scheme the event information or any other security related communications are forwarded through authenticated routing nodes. The routes used for communication are not fixed and cannot be predefined. Hence, it is difficult for the adversary to identify the route and perform selective forwarding attack without holding route authentication information. Moreover, it is impossible to forward falsified event report since each forwarding nodes verify the authenticity of the event report before forwarding the event report.

4.2.2.3. Resilient to node compromisation. In the proposed scheme node compromisation does not cause serious effects in communication. The adversary is unable to succeed in his actions by compromising a node. Even if an en-route node is compromised, it does not produce serious effect as no information can be revealed by an adversary through the compromised forwarding node. Security credentials used for protecting the event information is dynamic and cannot be exposed to the compromised node. Hence it is confirmed that data compromisation cannot be performed in the proposed scheme.

4.2.2.4. Resilient to traffic analysis attack. The identities of the node involved in communication are not exposed to any other nodes. Moreover, by means of the proposed hop-by-hop anonymous secure communication scheme encryption and decryption are done at each intermediate hop. This technique helps to maintain privacy of the information in transit. Also different hops may produce different encrypted output. Even though the encrypted information can be received by an adversary he may not be able to retrieve the original information. The strong secrecy achieved is due to the session key transport capability.

4.3. Comparison of functionality of the proposed and related schemes

In this section some comparisons are done based on the functions of the proposed and related schemes. Explanation about the functionality of the schemes is also presented. Table 2 shows the relationship between functionality of proposed scheme, BECAN [24] and SET-IBS [15].

Route criterion: Route criterions are used in routing mechanisms to select suitable forwarding nodes. In the proposed scheme link quality and residual energy of nearby sensor nodes are collected to determine suitable forwarding nodes. But in BECAN distance or hop count is used as a deciding factor and in SET-IBS route determination is through the residual energy of cluster members.

Authentication: used for access control and for transmitting data securely to neighbouring nodes. Authentication is done through authentic message segment in proposed scheme, MAC in BECAN and by generating and verifying digital signature in SET-IBS.

Key management: Cryptographic operation to ensure confidentiality. This is done with the help of symmetric secret key in the proposed scheme, asymmetric key generation and sharing in SET-IBS and non-interactive key pair in BECAN.

Privacy: Used to protect the location information of nodes involved in communication. The related schemes SET-IBS and BECAN are not following privacy preserving mechanisms. But the proposed scheme achieves all three kinds of anonymities.

Table 2
Comparison of functionality between proposed and other schemes.

Functionality	Proposed	SET-IBS	BECAN
Route criteria	Link quality, residual energy	Residual energy	Shortest path
Authentication	Authentication message	Digital signature	Message Authentication Code (MAC)
Key management	Symmetric key	Asymmetric key	Non interactive key pair
Privacy	Anonymity	Not applicable	Not applicable
Key freshness	Session key	Timestamp	Timestamp

Key refreshness: Keys used by the nodes are periodically refreshed to prevent cryptanalytic attack. In the proposed scheme key refreshness check is performed through the session key. Hence previous message cannot be replayed. In the related schemes BECAN and SET-IBS refreshness is verified through the timestamp value endorsed in each packet.

5. Simulation results and analysis

The performance of the proposed scheme is studied through simulation using NS2 and is compared with related schemes BECAN [24] and SET-IBS [15]. The comparison is made in terms of network lifetime, end-to-end delay, packet drop ratio, resilience against node capture, energy consumption in communication.

- *Network lifetime:* Network lifetime is defined as the time until the first sensor node along with the path runs out of energy. Efficiency in a routing mechanism is to prolong network lifetime.
- *Packet drop ratio:* Packet drop ratio is determined by the ratio of numbers of packets dropped or lost to the total number of packets sent by the source node.
- *Resilience against node capture:* Resilience rate of the network against node capture is determined by comparing the number of nodes captured with the fraction of total network communication that are exposed to the adversary.
- *End-to-end delay:* End-to-end delay is the time difference from the time a source node sends its data packet to the time the BS receives it.
- *Energy consumption:* The energy consumed for one round of communication from source to base station.

5.1. Simulation settings

This work is implemented over NS2, the network simulator [25]. A WSN of 200 sensor nodes are randomly deployed into $1000 \times 1000\ m^2$ regions of interest. All the sensor nodes are assigned to have same hardware and transmission power. The main objective of the simulation is to evaluate the performance of the proposed secure communication scheme in the presence of compromised nodes. The simulation results are studied by varying the count of compromised nodes and varying the number of forwarding nodes. The parameters used in simulation are tabulated in Table 3. Fig.2 shows the deployment of sensor nodes in an area of $1000 \times 1000\ m^2$ with a single BS.

5.2. Simulation results

The performance of the proposed scheme is studied using NS2, a network simulator popularly used in the evaluation of network performance. For performance evaluation the proposed RASP and is compared with related schemes BECAN and SET-IBS. The metrics for performance evaluation are: network lifetime, end-to-end delay, packet drop ratio, resilience against node capture, energy consumption for communication.

Fig.3 illustrates the network lifetime with respect to network size. It is shown that proposed scheme outperforms the related schemes. The network lifetime decreases as the number of nodes in the network increases. The proposed scheme

Table 3
Parameter settings for simulation.

Parameter	Value
Number of nodes	200
Number of compromised nodes	20–30
Initial energy for each sensor node	2 J
Transmission range	50 m
Time consumption for hash operation	1.5 ms
Number of forwarding nodes	1–24
Simulation time	180 s
Energy consumption for sending a packet	16.5 μJ
Energy consumption for receiving a packet	12.5 μJ

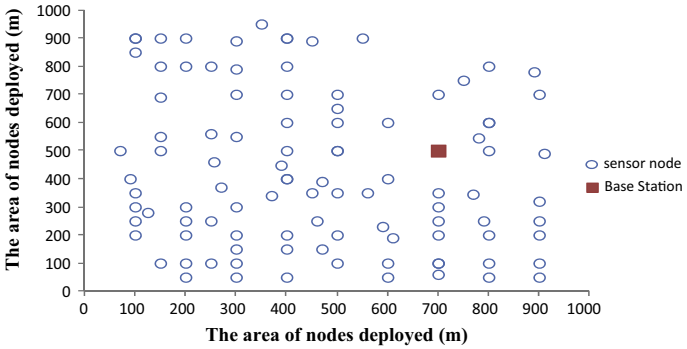

Fig. 2. Deployment of sensor nodes.

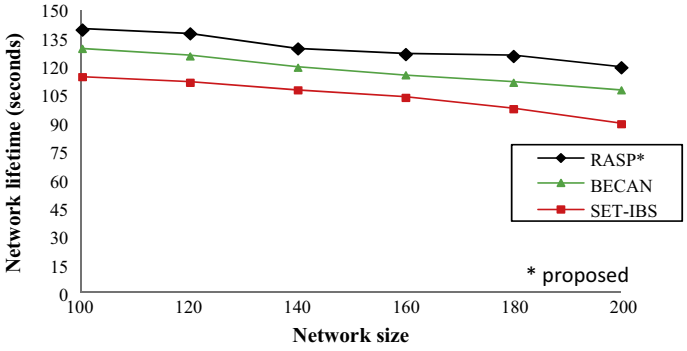

Fig. 3. Network lifetime as the network size increases.

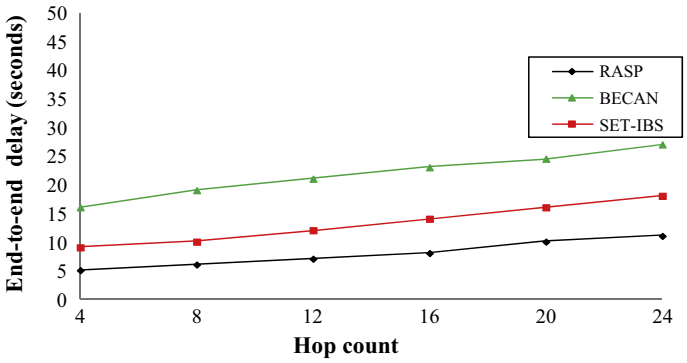

Fig. 4. Average delay in packet transmission from source to destination.

determines reliable and more efficient path to prolong network lifetime. But the schemes BECAN and SET-IBS transmit many messages in the network which increases energy consumption of forwarding nodes. Hence the network lifetime gets reduced. The proposed scheme outperforms the related schemes SET-IBS, BECAN as the network size increases from 100 nodes to 200 nodes.

Fig.4 shows a comparison done in terms of end-to-end delay with differing hop count in the presence of 20 compromised nodes. It is assumed that compromised node can eavesdrop and monitor the network traffic. Then time required for end-to-end communication with the intervention of adversary is determined. It can be seen clearly that average time delay caused by the proposed scheme is less than that of the related schemes. This is due to the fact that in the SET-IBS more control messages are exchanged for ensuring security. The maximum delay caused in BECAN is due to large number of operations performed in generating and verifying the authentication message by the forwarding nodes.

Fig.5 shows the packet drop ratio in the presence of compromised nodes. In the proposed scheme though the compromised nodes can eavesdrop the packet, they are unable to perform any other disruptions over the received packet. Hence most of the packets are delivered successfully to destination and the drop ratio is very much reduced. But the related

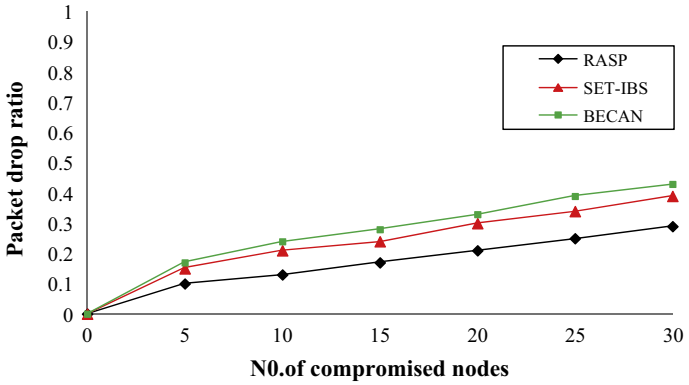

Fig. 5. Packet drop ratio the with the increase of compromised nodes.

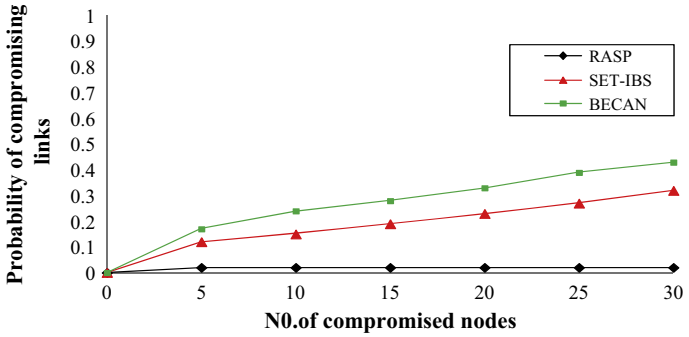

Fig. 6. Resilience of node capture attack.

schemes BECAN and SET-IBS are susceptible to traffic analysis attack thereby adversary is modify the packet on transit. This results in unsuccessful delivery of packets. Hence the drop ration gets increased.

Fig.6 illustrates the probability of compromising links as a function of absolute number of compromised nodes. It is assumed that once a sensor node is captured, the adversary can read all security credentials in it. In proposed scheme the session keys and secret keys are established on demand. The source and destination share a unique one time secret key. The capture of sensor nodes has no impact on the secure links between other uncompromised nodes. But in related scheme BECAN capturing a sensor node reveals the common key shared with neighbour nodes resulting in compromisation of uncompromised nodes. Hence the chance for compromising the links gets increased. The probability of compromising increases as the chance for sharing keys gets increases.

Energy consumption for one round of communication from source to BS for different schemes is represented in Fig 7. In this figure energy consumption for transmission is represented along with the *X*-axis and count of intermediate nodes along the path is represented through the *Y*-axis. It is assumed that all the intermediate nodes and the source node involved in

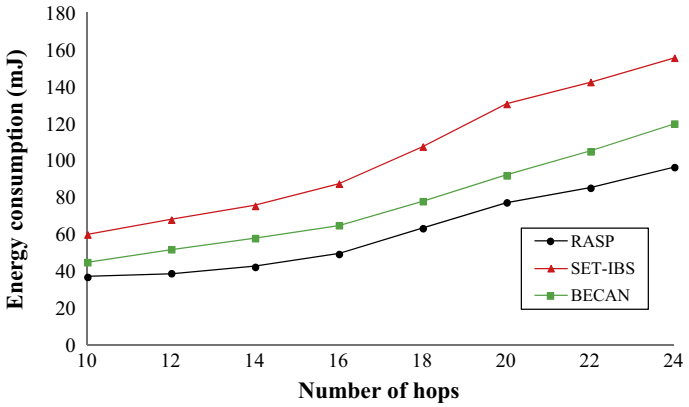

Fig. 7. Energy consumption for single round of communication.

communication have the keying materials for establishing the security features. In addition the protocols are allowed to perform perfect communication without packet loss. The results are generated by varying the number of hops between source and BS. The related schemes BECAN and SET_IBS exchange many messages and involve the use of many keys to ensure security. Hence the energy consumed while establishing communication by the related schemes is more compared to proposed scheme.

6. Conclusion

Reliable data transmission is essential to prolong the overall lifetime of the WSNs. The proposed mechanism achieves reliability by favouring maximum residual energy and high link quality for nodes involved in routing. Further, the proposed scheme protects the communication from passive and active attacks. In comparison with other secure communication schemes, RASP has the following advantages. (i) It determines trust worthy nodes for forwarding the packets. (ii) It uses one time secret key to encrypt the data and is highly resilient to data compromisation. (iii) It does not exchange control message for providing security services for the data in transit. Hence reduces the extra energy consumption during data transmission. (iv) It prevents the exposure of identities of nodes involved in communication thereby protects the packet from traffic analysis attack. The performance of the proposed scheme is evaluated based on several metrics and the simulation results demonstrated the effectiveness of the proposed secure communication framework. By evaluation through simulation it has been determined that, the proposed scheme achieves high reliability in communication with increased network lifetime, high security against passive and active attacks.

References

[1] Akyildiz IF, Su W, Sankarasubramanian Y, Cayirci E. A survey on sensor networks. IEEE Commun Mag 2002;40(8):102–14.
[2] Annlin Jeba SV, Paramasivan B. False data injection attack and its countermeasures in wireless sensor networks. Eur J Sci Res 2012;82(2):248–57.
[3] Annlin Jeba SV, Paramasivan B. Energy efficient multipath data transfer scheme to mitigate false data injection attack. Comput Electr Eng 2013;39(6):1867–79.
[4] Nezhad AA, Miri A, Makrakis D. Location privacy and anonymity preserving routing for wireless sensor networks. J Comput Networks 2008;52(18):3433–52.
[5] Pandey Manjusha, Verma Shekhar. Privacy provisioning in wireless sensor networks. J Wireless Pers Commun; Springer 2014;75(2):1115–40.
[6] Haas Zygmunt J, Yang Lin, Liu Meng-Ling, Li Qiao. Current challenges and approaches in securing communication for sensors and actuators. The Art of Wireless Sensor Networks Signals and Communication technology, vol. 1. Berlin, Heidelberg: Springer Verlag; 2014. p. 569–608.
[7] Kalyani P, Chellappan C. Analysis of security and key management schemes for authenticated broadcast in heterogeneous wireless sensor networks. J Commun Comput Inf Sci 2011;169:580–7.
[8] Javan Bakht Masoumeh, Erfani Hossein, Haj Hamid, Javadi Seyyed. Key predistribution scheme for clustered hierarchical wireless sensor networks based on combinatorial design. J Secur Commun Networks; Wiley 2014;7(11):2003–14.
[9] Annlin Jeba SV, Paramasivan B. Enhanced efficient group key transfer scheme for wireless sensor networks. Sci Res Essays Acad J 2012;7(47):4060–70.
[10] Traynor P, Choi H, Cao G, Zhu S, Porta TL. Establishing pair-wise keys in heterogeneous sensor networks. In: Proceedings of the 25th IEEE conference on computer communications (INFOCOM); 2006. p. 1–12.
[11] Liu D, Ning P. Improving key pre-distribution with deployment knowledge in static sensor networks. ACM Trans Sen Networks (TOSN) 2005;1(2):204–39.
[12] Yasmin R, Ritter E, Wang G. An authentication framework for wireless sensor networks using identity-based signatures. In: The proceeding of IEEE CIT; 2010.
[13] Gaikwad Shital Y, Kulkarni UV. Comparative analysis of hop-to-hop and end-to-end secure communication. Int J Adv Res Technol 2013;2(7):473–7.
[14] Oliveira LB, Ferreira Adrian, Vilaca Marco A. SecLEACH-on the security of clustered sensor networks. J Sig Process 2007;87:2882–95.
[15] Lu Huang, Li Jie, Guizani Mohsen. Secure and efficient data transmission for cluster-based wireless sensor networks. IEEE Trans parallel Distrib Syst 2013:1–10. issue: 99.
[16] Yu Hong, He Jingsha, Zhang Ting, Xiao Peng. Enabling end-to-end secure communication between wireless sensor networks and the internet. World Wide Web, Internet Web Inf Syst, Springer 2013;16(4):515–40.
[17] Wen Fengtong, Li Xuelei. An improved dynamic ID-based remote user authentication with key agreement scheme. Comput Electr Eng 2012;38(2):381–7.
[18] Ye F, Luo H, Lu S, Zhang L. Statistical en-route detection and filtering of injected false data in sensor networks. In: Proceedings of IEEE INFOCOM. vol. 4; 2004. p. 2446–57.
[19] Yu Zhen, Guan Yong. A dynamic en-route filtering scheme for data reporting in wireless sensor networks. IEEE/ACM Trans Networking 2010;18(1):150–64.
[20] Ren K, Lou W, Zhang Y. LEDS: providing location aware end to end data security in wireless sensor networks. IEEE Trans Mob Comput 2008;7(5):585–98.
[21] Gu Wenjun, Dutta N, Chellappan S, Bai Xiaole. Providing end-to-end secure communications in wireless sensor networks. IEEE Trans Network Serv Manage 2011;8(3):205–18.
[22] Park Jeong-Hyp, Jung Yong-Hoon. A privacy technique for providing anonymity to sensor nodes in a sensor network. Ubiquitous computing and multimedia applications CCIS, vol. 150. Springer; 2011. p. 327–35.
[23] Shao M, Yang Y, Zhu S, Cao G. Towards statistically strong source anonymity for sensor networks. In: The proceedings of IEEE INFOCOM; 2008 p. 51–5.
[24] Lu R, Lin X, Zhu H, Liang X. 'BECAN: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks. IEEE Trans Parallel Distrib Syst 2012;23(1):1–13.
[25] Fall K, Varadhan K. The ns manual. UC Berkeley and LBL and USC/ISI and Xerox PARC; 2007.

S.V. Annlin Jeba: Obtained Bachelor of Engineering and Master of Engineering in Computer Science and Engineering from Anna University, Chennai. She received her PhD from Anna University. She is working as Associate Professor in C.S.I. Institute of Technology, Tamil Nadu, India with 14 years of teaching experience and done research in the area of wireless sensor networks. She has more than 15 publications in international journals and conferences.

R. Suresh Kumar: Received the Master degree in Mathematics under MS University, India. He is recently working as Associate Professor in C.S.I. Institute of Technology, TamilNadu, India with 18 years of teaching experience. His area of interest is Near rings and Graph theory.