Ensuring Basic Security and Preventing Replay Attack in a Query Processing Application Domain in WSN

Amrita Ghosal[1], Subir Halder[1], Sanjib Sur[2], Avishek Dan[2], and Sipra DasBit[2]

[1] Dept. of Comp. Sc. & Engg, Dr. B. C. Roy Engineering College, Durgapur, India
ghosal_amrita@yahoo.com, subir_ece@rediffmail.com
[2] Dept. of Comp. Sc. & Tech., Bengal Engineering and Science University, Shibpur, India
{sanjib.sur11,avishekdan}@gmail.com, siprad@hotmail.com

Abstract. Nodes in a wireless sensor network are susceptible to various attacks primarily due to their nature of deployment. Therefore, providing security to the network becomes a big challenge. We propose a scheme considering cluster architecture based on LEACH protocol to build a security mechanism in a query-processing paradigm within wireless sensor network. The scheme is capable of thwarting replay attack while ensuring essential properties of security such as authentication, data integrity and data freshness. Our scheme is lightweight as it employs symmetric key cryptography with very short-length key. We simulate our scheme to show its efficacy of providing basic security to the network as well as detecting replay attack in the sensor network. Further we compare our scheme with one of the existing schemes taking packet loss and packet rejection ratio as performance metrics.

Keywords: replay attack, denial of service attack, authentication, data integrity, data freshness.

1 Introduction

The advent of efficient short range radio communication and advances in miniaturization of computing devices have given rise to strong interest in wireless sensor networks (WSNs) [1]. A wireless sensor network (WSN) consists of a large number of small, battery-powered [2], [3] wireless sensor nodes. The nodes are distributed in ad-hoc fashion and process sensing tasks. A sensor network may be deployed in hostile environments where there can be malicious attackers. On the other hand, the WSNs are used in critical application domain e.g. defense, medical instrument monitoring. Therefore, securing the activities of WSNs is of utmost importance.

These WSNs are prone to attacks [4], [5] due to their nature of deployment in an unattended environment and also due to the broadcast nature of the medium. One such attack is Denial of service (DoS) attack [6] that possesses a great threat to wireless sensor network environment. One form of DoS attack attempts to disrupt the network service, may be by blocking communication between nodes. The other form of DoS attack is the path-based DoS (PDoS) attack where the network is flooded with bogus packets along a multi-hop data delivery path [7]. The packets are continuously

D. Taniar et al. (Eds.): ICCSA 2010, Part III, LNCS 6018, pp. 321–335, 2010.

replayed back to the sink node. This attack is known as replay attack. However, the objective of both types of such attacks is to eliminate or diminish the network performance and thereby hamper the working of the whole system. In replay attack, because of the broadcast nature of sensor networks, an adversary eavesdrops on the traffic, injects new messages and replays/changes old messages.

Many works are so far reported towards the solution of various forms of DoS attack. Deng et al. [7] have considered a type of DoS attack along a multihop data delivery path. As WSNs are generally tree structured, so an attack on the nodes of a path also affects the branches connected to that path. A one way hash chain mechanism has been proposed by the authors to prevent such path based DoS attacks and protect end to end communication along a multihop data delivery path. Here an OHC (One way Hash Chain) number is added with each message packet leading to an extra overhead of 8 bytes per packet. These 8 bytes of additional overhead is a major constraint for a resource constrained sensor mode.

Authors in [8] have proposed an authentication protocol capable of resistance against replay attacks and other DoS attacks. But the scheme uses symmetric keys where keys are shared by sensor nodes and therefore a compromised node can send forged messages which may possess a great security threat to the network.

Perrig et al. [9] have used RC5 algorithm for encrypting messages which means a lot of computations have to be done. Here the μ TESLA protocol is used for secure broadcast of messages and an 8-byte Message Authentication Code (MAC) is used by each node for verification along the communication path. However, exchange of huge authentication information is a real bottleneck for the resource-constrained WSN. Moreover a node must have prior knowledge of all the nodes along its path.

The authors in [10] have devised a mechanism to prevent replay attacks. Here it is considered that the packets used for time-synchronization of any two nodes are replayed. A receiver-receiver model for time synchronization has been considered where a reference node broadcasts beacon message to all its neighbours. Based on the arrival time of the beacon message the receiving nodes adjust their clocks. A time offset is calculated based on the difference between the recording times of the beacon message by these receiving nodes. The time offsets are exchanged between the receiving nodes to calculate a threshold value which is the difference between the two time offsets of two nodes. But the arrival of a beacon message at a node can be delayed by certain factors leading to gross errors while deriving the time required for synchronization between the nodes. Moreover, by not using global time synchronization model a large overhead has been introduced as huge number of time offsets need to be computed by the nodes.

Dong et al. [11] have proposed the use of hash chains in their work where each node combines the hash value with its own node-id and forwards this combined value to its next higher hop count node. The receiving node is able to detect replay attacks by observing the combined value of node-id and hash value. But the computation of all these values by nodes takes significant amount of time.

Soroush et al. [12] have developed a scheme to defend replay attacks where a monotonically increasing counter is maintained to keep track of old replayed messages. But here each node maintains a counter to store the timing information of all other nodes which requires a large amount of memory leading to a major bottleneck for memory- constrained sensor nodes.

In this paper we propose a secured query processing scheme in WSN with a target to build a security mechanism from within a query-driven application environment. The proposed security mechanism gives a solution of replay attack while ensuring authentication, data integrity and data freshness.

The rest of the paper is organized as follows. In section 2 system model along with a brief description of the present work is given. A detailed description of the scheme is given in section 3. Section 4 gives the performance evaluation of the proposed scheme and also the comparative study between the proposed scheme and another scheme. Concluding remarks and future scope has been stated in section 5.

2 System Model

An attack [6] is defined as an attempt to gain unauthorized access to a service, resource, or information, or the attempt to compromise integrity, availability, or confidentiality. DoS is one type of attack which hinders communication among the sensor nodes. The present work considers replay attack, which is one form of path based DoS (PDoS) attack. If there is a PDoS attack, the network gets flooded with bogus packets along a multi-hop delivery path [7]. The occurrence of bogus packets in the network is due to the replaying of packets by adversaries leading to replay attack. So PDoS attacks in the network may result in replay attacks.

The system model in the present work considers clustered network architecture based on LEACH protocol [13]. In this architecture nodes organize themselves into local clusters with one node acting as the cluster head (CH). LEACH performs local data fusion to reduce the amount of data sent from the clusters to the base station/ sink. Once all the nodes are organized into clusters, each CH assigns a time slot (TDMA schedule) for the member nodes in its cluster. The member nodes sense data and transmit data to the cluster head nodes that are located at one hop distance away from them. The cluster head nodes transmit the same to the base station after receiving data from their member nodes.

The present work considers a query-driven application platform where base station generates query messages and broadcasts the query. Cluster heads receive the broadcasts query and start the registration process to authenticate their respective member nodes. Once the registration phase is over, the CHs forward the query messages to their members. Depending on the nature of queries, specific member nodes send response-packets.

The objective of the proposed scheme named as Secured Query Processing Scheme (SQPS) is to ensure basic security in general and prevent replay attack in particular while working for a query-driven application. The essential properties [14] of a WSN required for maintaining basic security within the network are:

- Authentication- A sensor network must be able to differentiate between data coming from reliable sources and those coming from adversaries.
- Data Integrity- The received data should not be tampered during communication between the sender and the receiver.
- Data Freshness- The data received at a particular time should be current data and not old data which may be replayed by adversaries.

3 The Scheme

In this secured query processing scheme as shown in figure 1, periodically queries are broadcast from base station. The process begins as soon as the cluster heads receive queries from base station. The scheme has two phases-

- Registration Phase
- Query Response Phase

3.1 Registration Phase

This phase is used for registering member nodes by the respective cluster head nodes. The objective of this phase is to register only the authenticated nodes. Moreover the phase provides a mechanism that will help a CH to ensure data integrity and data freshness during query processing phase. Upon receiving a query from the base station, cluster heads initially broadcast registration packet.

The registration packet contains 8 bits including '0' as MSB. This MSB differentiates between a registration packet and a query packet sent by the cluster heads. As mentioned in section 2, each member node is allotted a particular time slot which is used for sending a registration response packet to the cluster head corresponding to the registration packet and also for receiving identification (node-id) for the member node from the cluster head for continuing the query processing session. On receiving the registration packet, the respective member nodes decide the number of bits to be shifted and accordingly left shift the bits of registration packet. Then the nodes generate registration response packet including left-shifted registration packet (8 bit), number of bits left shifted (3 bit), and present time-stamp (12 bit). The key used here is the number of left shifted bits. Symmetric key cryptography is used as the same key is used for encryption and decryption of the data packets. Symmetric key cryptography is beneficial for sensor networks as less computation has to be done and memory requirement is also minimized. Here, though the key is being sent along with the registration packet it will not be possible for any adversary who captures or eavesdrops the contents of the packet to decipher which bits in the packet refer to the key. Moreover in traditional networks the adversary performs some computations to obtain the key used in the network; this is not possible in case of sensor networks as the adversary nodes are also equipped with less computational power. The present time-stamp indicates the time when a member node sends a reply packet in response to the registration packet. The time-stamp is represented in minutes and seconds.

Immediately after receiving a registration response packet from one of its member node, the CH right shifts the reply packet designated number of times. The number of bits to be right shifted is same as the number of bits the registration packet is left shifted and it is provided as control data in the registration response packet itself. If the CH can retrieve the original registration packet after right shifting the received registration response packet, the member node is considered as an authenticated and registered node. Upon authenticating a member node, the CH generates a node-id and sends it to the member node at the same time slot of authenticating and registering the member node. Once the registration of a member node is successful, the CH stores this information.

3.1.1 Encryption at Registration Phase

Let us consider an 8-bit binary registration packet as S= $m_7 \ldots m_0$, where MSB is m_7 and LSB is m_0. The registration packet is broadcast by cluster head at a particular time slot. Time slots are assigned to member nodes according to TDMA schedule. On receiving the registration packet S, member nodes randomly choose the shift bit B for left shifting. If B is 100, S is encrypted as $m_3m_2m_1m_0m_7m_6m_5m_4$ (S'). Accordingly a 3-tuple registration response (RR) packet is formed by the member node as $(S''$, $B, T_{MN\_present})$, where $T_{MN\_present}$ is present time-stamp.

3.1.2 Decryption at Registration Phase

Upon receiving the encrypted registration response packet $(S'', B, T_{MN\_present})$ from a member node, the cluster head performs the reverse process of encryption to get back the original registration packet. So S' is right shifted B times and converted to S''. After decrypting, if S'' matches with S, the cluster head accepts the registration packet and authenticates the corresponding member nodes.

3.1.3 Data Stored by Cluster Head

Once the cluster head authenticates a member node, it generates an identification (node-id) for the member node and stores a 6-tuple data (node-id, S, S', B, $T_{MN\_present}$, $T_{MN\_previous}$) for the member node where S', B, $T_{MN\_present}$ is RR (packet sent by the node designated by node-id), S is the original registration packet and $T_{MN\_previous}$ is a time-stamp which is set to null initially.

3.1.4 Data Stored by Member Node

Once a member node gets its node-id from the cluster head during registration, the member node stores 3-tuple (node-id, B, $T_{MN\_present}$) data.

3.1.5 Algorithm for Registration

```
Begin
// Action executed by cluster heads (CHs)
CH broadcasts 8-bit registration packet (S) at time t
// Actions executed by member nodes (MNs)
On receiving S at time (t+1)
for i=t+1, i<=t+n, i++
    left shift S to obtain $S'_i$        /* i^th member node ($MN_i$) encrypts S by left shifting it by $B_i$-bit which is arbitrarily chosen by $MN_i$ to obtain $S'_i$ */
    Generate $RR_i$                       /* $MN_i$ generates 3-tuple registration response packet RR($S'_i$, $B_i$, $T_{MN_i\_present}$) */
    Send $RR_i$ to CH
// Actions executed by cluster head (CH) on receiving $RR_i$ from $MN_i$
```

```
right shift $S'_i$ to obtain $S''_i$      /* CH decrypts $S'_i$ by right shifting it by
                                          $B_i$-bit to obtain $S''_i$ */
if $S''_i = S$ then
    $RR_i$ is authentic                   /* registration response packet $RR_i$ is
                                          authentic */
    accept $RR_i$                         /* CH accepts registration response packet
                                          $RR_i$ */
    generate node-id for $MN_i$
    send node-id to $MN_i$
    store 6-tuple data                    /* 6-tuple data: ($node-id_i$, $S$, $S'_i$, $B_i$,
                                          $T_{MN_i\_present}$, $T_{MN_i\_previous}$)*/
// Action executed by $MN_i$ on receiving $node-id_i$
    store 3-tuple data              /*3-tuple data: $node-id_i$, $B_i$, $T_{MN_i\_present}$ */
else
    reject $RR_i$
end if
end for
End
```

Node authentication is one of the major parameters of network security. The registration phase of the present scheme is able to ensure this part of security.

3.2 Query Response Phase

In the event of query processing, the base station broadcasts query. Upon receiving the query, a CH starts registration phase. Once the registration phase is over (section 3.1), the CH broadcasts the query for its member nodes. Depending on the query, specific member nodes send response and cluster head nodes forward the responses to base station. For example, if the query is related to temperature, then member nodes responsible for sensing temperature provide response to the query.

Query packet is of 8 bits. The MSB bit of the query packet is always 1, to distinguish between registration packet and query packet. So, 128 different queries can be generated with the remaining 7 bits of the query packet.

3.2.1 Encryption at Query-Response Phase

On receiving query packet member nodes respond to the query in the form of a query response (QR) packet that contains 5-tuple (node-id, m, m', $T_{MN\_present}$, $T_{MN\_previous}$) where m is an 8-bit response message for the corresponding query and m' is left shifted (B times) message. Further, $T_{MN\_present}$ and $T_{MN\_previous}$ are present time stamps when the member node is sending the response packet for the query and previous time stamp of last communication (packet exchange) between member node and CH respectively. To start with, $T_{MN\_present}$ of the 3-tuple data stored by the member node at registration phase replaces $T_{MN\_previous}$.

3.2.2 Data Stored by Cluster Head

After receiving query response packet from member node, the cluster head updates the 6-tuple data stored at registration phase. During registration phase the stored 6-tuple data was (node-id, $S, S', B, T_{MN\_present}, T_{MN\_previous}$). During query response phase, S and S' attributes are replaced by m and m' respectively. $T_{MN\_previous}$ which contained null value during registration phase is now replaced by $T_{MN\_present}$ which was stored during registration phase and $T_{MN\_present}$ is replaced by the time when the query response packet is being sent by the member node.

3.2.3 Decryption at Query-Response Phase

Cluster head on receiving the QR packet, finds the node-id of the member node from the packet. Then to decrypt the encrypted message m', the CH right shifts m', B times where B is found from the stored tuple corresponding to the node-id of the member node. The m' is converted to m'' after decryption. Once the CH decrypts the message part of the QR packet, it checks for data integrity, data freshness and replay attack.

3.2.4 Check for Data Integrity

If it is found that the decrypted message m'' is same as the original message m, data integrity is preserved.

3.2.5 Check for Replay Attack and Data Freshness

In replay attack the malicious node repeats the already sent packets and results in energy exhaustion of nodes and eventually collapse of the network. With the help of two attributes $T_{MN\_present}$ and $T_{MN\_previous}$ stored at cluster head corresponding to every registered/ authenticated member nodes, replay attack is detected. The cluster head compares the $T_{MN\_present}$ and $T_{MN\_previous}$ of an entry corresponding to a member node and if $T_{MN\_present}$ stored by it and the $T_{MN\_previous}$ in QR is equal, then it can be ensured that no replay attack has taken place and data freshness is preserved.

If a malicious node attempts to send query response packet posing as an authenticated member node, cluster head rejects the packet. Due to this unauthorized attempt, an authorized node's TDMA time slot will be consumed and as a result of which a packet to be sent by the authorized node is lost. Therefore, there may be two distinct effects of malicious attempt- one is packet loss and the other is packet rejection.

3.2.6 Algorithm for Query Response

```
Begin
// Action executed by cluster head (CH)
Broadcasts query packet received from base station at time (t+n+1)
// Actions executed by member nodes (MNs)
On receiving query packet at time (t+n+2)
for i= t+n+2, i<=t+2n+2, i++
    send 5-tuple $QR_i$ to CH        /* $i^{th}$ member node sends query response packet, $QR_i$ ( $node-id_i, m_i, m'_i$ ( $m_i$ left shifted by $B_i$ bit)), $T_{MN_i\_present}, T_{MN_i\_previous}$ )to CH */
    right shift $m'_i$ to obtain $m''_i$        /* CH decrypts $m'_i$ by right shifting it by $B_i$ -bit to obtain $m''_i$ */
    if $m''_i = m_i$ then        /* check for data integrity */
        accept        /* data integrity is maintained */
    else
        reject $QR_i$        /* data integrity is violated */
    end if

        if CH.$T_{MN_i\_present}$ =
        QR.$T_{MN_i\_previous}$ then        /* CH compares $T_{MN_i\_present}$ stored in it with $T_{MN_i\_previous}$ in $QR_i$ */
            accept $QR_i$        /* no replay attack is detected */
            update its (CH's) stored data
            corresponding to $MN_i$        /* replaces S by $m_i$, $S'_i$ by $m'_i$, $T_{MN_i\_previous}$ by $T_{MN_i\_present}$, $T_{MN_i\_present}$ by $T_{MN_i\_present}$ of $QR_i$ */

// Action executed by CH on receiving $QR_i$
        else
            reject $QR_i$        /* CH rejects query response packet $QR_i$ */
        end if
end for
End
```

The present scheme is based on LEACH protocol which is an internationally accepted standard protocol. It adds security feature to the LEACH protocol in a lightweight manner involving shifting of bits. The scheme is implementable as computations for shifting of bits is highly implementable in sensor nodes e.g. mica-2 motes.

3.3 Diagrammatic Representation of the Scheme

The entire scheme is illustrated with the help of an activity diagram shown in Figure 1.The diagram shows how a cluster with n number of nodes and one cluster head works. To be more specific, it shows communication among different components of a wireless sensor network and control flow among various computational modules within the components of the network. Broadcast communication from cluster head is shown by lightning symbol whereas unicast communication between cluster head and member nodes and control flows are shown by solid lines with arrowhead. All communication symbols are labeled to make understand the content of the packet along with the timestamp at which it is being sent. For example, one broadcast communication labeled by RB_t means registration packet has been broadcast at time t. Timestamp helps to know the steps of operations visibly.

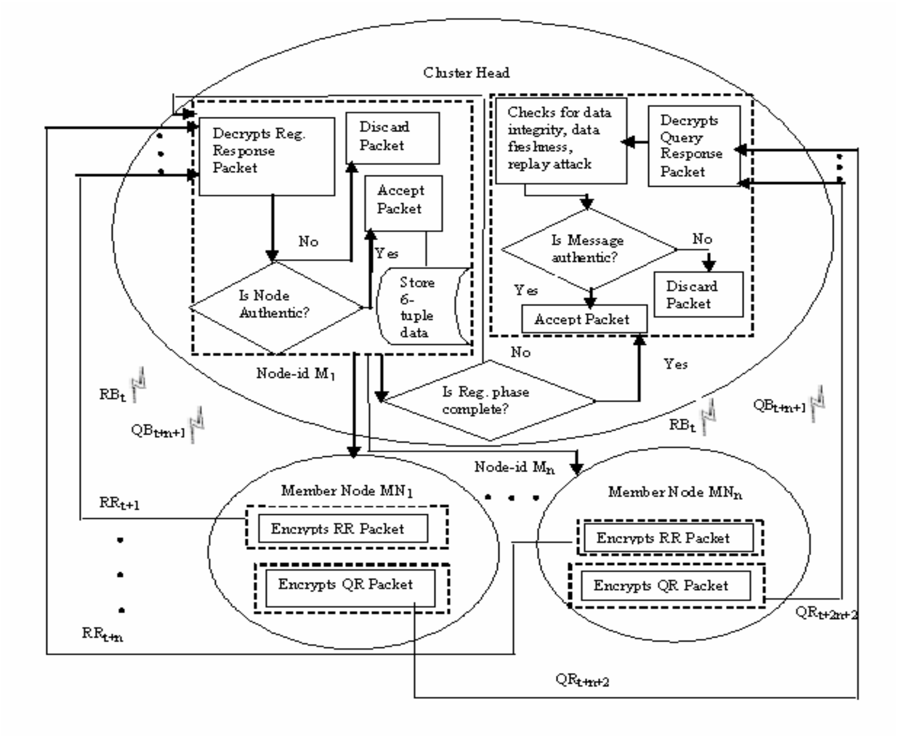


Fig. 1. Activity diagram of the proposed scheme (SQPS)

The notations used in Figure 1 has been described below-

RB_t – Registration Packet broadcast at time t by cluster head.

RR_{t+1} – Registration response packet transmitted at time t+1 by member node M_1.

RR_{t+n} – Registration response packet transmitted at time t+n by member node M_n.

Node – id M_1 – Node-id of member node M_1 transmitted at time t+1 by cluster head.

$\text{Node}-\text{id}\, M_n$ – Node-id of member node M_n transmitted at time t+n by cluster head.
QB_{t+n+1} – Query packet broadcast at time t+n+1 by cluster head.
QR_{t+n+2} – Query response packet transmitted at time t+n+2 by member node M_1.
QR_{t+2n+2} – Query response packet transmitted at time t+2n+2 by member node M_n.

4 Performance Evaluation

The effectiveness of the proposed security scheme reported in the earlier section is evaluated through simulation.

4.1 Simulation Environment

Simulation is performed using MATLAB (version 7.1). We consider 500 nodes in the network and number of malicious nodes is varied from 25 to 100.

Performance of the scheme is evaluated based on the following two metrics:

Authentication Rate – Number of authenticated nodes / total number of nodes in the network.
Data freshness (%) – (Number of received packets containing current data / total number of packets sent) x 100.
The relevant parameters and their associated values are listed below in Table 1-

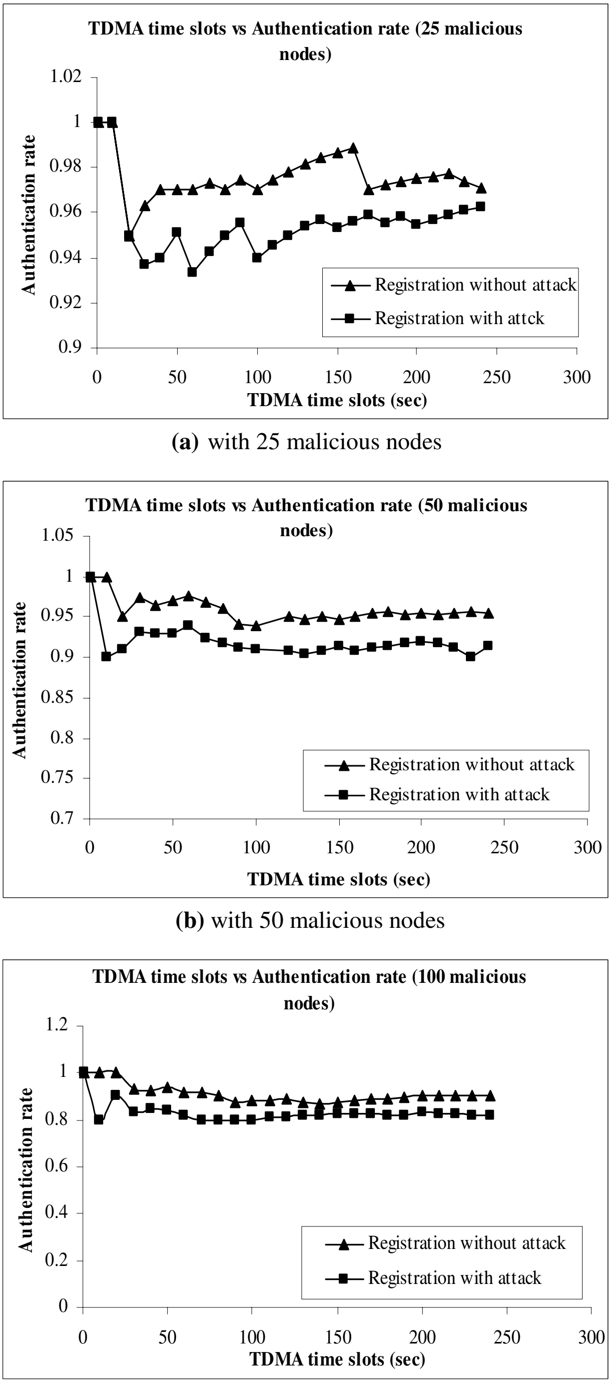
Table 1. Parameters and their corresponding values used in simulation

Parameters	Value
Initial Energy ($E_{initial}$)	2 J
Network area (user input)	25m × 25m to 100 m × 100 m
Communication range of sensor (R_c)	160 m
Sensing range of sensor (R_s)	80 m

In presence of replay attack, data freshness is affected. In other words, if replay attack can be considered as a cause, data freshness is an effect. Therefore, the metric, data freshness is measured to cover analysis on both the security parameters replay attack and data freshness. Authentication rate is computed to cover another security parameter i.e. authentication. No separate experiment is carried out to measure data integrity as violation of data integrity due to presence of malicious node does not arise.

4.2 Simulation Results

Authentication rate is measured and plotted with time in Figure 2 for varying number of malicious nodes. Two sets of experiments are conducted to compute authentication rate.



(a) with 25 malicious nodes

(b) with 50 malicious nodes

(c) with 100 malicious nodes

Fig. 2. Authentication rate over a period of time

In one set of experiment, we consider that malicious nodes are present and attempt to participate for sending data but stop participation once it is refused to do so. Results are plotted in Figure 2 for varying number of malicious nodes and designated as ‘without attack’. In the other set of experiment, malicious nodes attempt to send data repeatedly resulting in replay attack. Results of the same are plotted and designated as ‘with attack’.

We observe that in all the cases of Figure 2 ((a), (b), (c)) results ‘with attack’ show a fall of authentication rate compared to the results of ‘without attack’. This signifies presence of replay attack from malicious nodes. Further, if we compare results of all the plots ((a), (b), (c)), it is observed that authentication rate decreases with increase in number of malicious nodes.

Figure 3 shows percentage of data freshness over a period of time in presence of malicious nodes. Results in presence of 25 malicious nodes show that average data freshness is near about 96% whereas its values are 88% and 81% for 50 and 100 malicious nodes respectively. The results indicate that data freshness is inversely related to the number of malicious nodes present in the network.

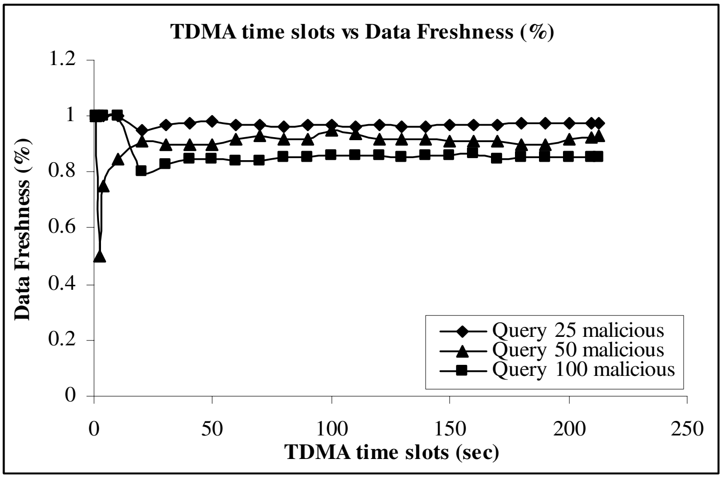


Fig. 3. Data freshness (%) over a period of time

4.3 Comparative Study

Due to unavailability of an existing suitable work so that our scheme can be compared based on all the security parameters considered here, we have chosen a work [11] on secured routing scheme to compare packet loss and data packet rejection ratio as comparison metrics as defined below.

Packet loss (%) – Total number of received packets by a CH / total number of packets sent by the member nodes.

Packet rejection ratio (%) – Total number of received packets by a CH containing tampered data / total number of packets sent by the member nodes.

Packet loss and packet rejection ratio (%) are computed and plotted for varying number of malicious nodes in Figure 4 and Figure 5 respectively.

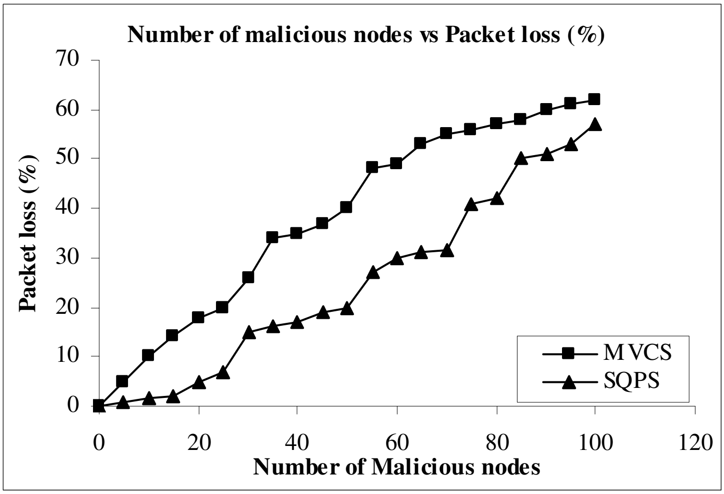


Fig. 4. Packet loss by varying number of malicious nodes

The figures also show the results for secured routing scheme named as MVCS (mitigating attack against virtual coordinate system) [11]. We observe that packet loss (Figure 4) increases with the increase of malicious nodes for both the schemes. However, in our scheme (SQPS), packet loss is about 16% less than MVCS for up to 25 numbers of malicious nodes. For 25 to 85 numbers of malicious nodes packet loss in SQPS is about 20% less than MVCS and this onwards packet loss is about 16% less in SQPS. Summarily, it can be said that packet loss in SQPS is less than MVCS for all sets of values of malicious nodes.

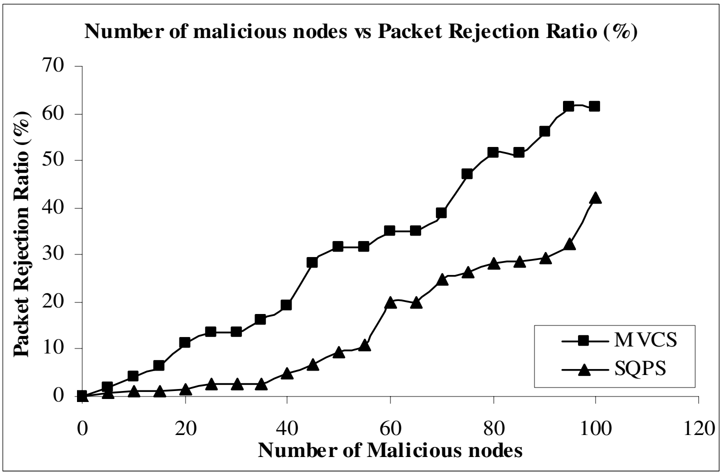


Fig. 5. Packet Rejection (%) by varying number of malicious nodes

Further we observe that packet rejection ratio (Figure 5) increases with the increase of malicious nodes for both the schemes. But in our scheme (SQPS), packet rejection is about 10% less than MVCS for up to 25 malicious nodes. For 25 to 100 malicious nodes packet rejection ratio in SQPS is 20% less than MVCS and this trend continues. So it can be inferred that packet rejection in SQPS is less than MVCS for all sets of values of malicious nodes. As all the member nodes' identities are verified through registration phase, there is very little chance that a malicious node is able to steal the identity of a legitimate node and passes through registration phase. That is why SQPS packet rejection ratio is lower than MVCS.

5 Conclusion

In this paper, we have proposed a scheme to defend replay attacks on nodes of WSN as well as preserve the essential basic security properties such as authentication, data integrity and data freshness of such a network. The scheme is designed in such a manner that no malicious node can take part in actual query processing thereby ensuring authentication.

Moreover, as there is no participating malicious node, violation of data integrity due to attack has been eliminated. However, a malicious node can attempt to participate stealing some time slots due to which there may be some packet loss. The merit of the scheme lies on the fact that simple symmetric key cryptography has been used to maintain security making the solution very lightweight. We have substantiated our claims by simulating the scheme in presence of attacks. Finally the scheme is compared with one of the existing routing schemes considering packet loss and data packet rejection ratio as comparison metrics. Results show our scheme outperforms the existing one.

As a future extension, the scheme may be made more realistic considering cluster head nodes are also vulnerable to attack. Further enhancement may be done to make it applicable for continuous data-flow application domain as well.

References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks. IEEE Communications Magazine 40(8), 102–114 (2002)
2. DasBit, S., Ragupathy, R.: Routing in MANET and Sensor Network- A 3D position based approach. Journal of Foundation of Computing and Decision Sciences 33(3), 211–239 (2008)
3. Halder, S., Ghosal, A., Sur, S., Dan, A., DasBit, S.: A Lifetime Enhancing Node Deployment Strategy in WSN. In: Lee, Y.-h., et al. (eds.) FGIT 2009. LNCS, vol. 5899, pp. 296–308. Springer, Heidelberg (2009)
4. Ghosal, A., Halder, S., DasBit, S.: A Scheme to tolerate Jamming in multiple nodes in Wireless Sensor Networks. In: Proceedings of Wireless VITAE, pp. 948–951. IEEE Press, Los Alamitos (2009)
5. Ghosal, A., Halder, S., Chatterjee, S., Sen, J., DasBit, S.: Estimating delay in a data forwarding scheme for defending jamming attack in wireless sensor network. In: Proceedings of 3rd International Conference NGMAST, pp. 351–356. IEEE CS Press, Los Alamitos (2009)

6. Wood, A.D., Stankovic, J.A.: Denial of Service in Sensor Networks. IEEE Computer 35(10), 54–62 (2002)
7. Deng, J., Han, R., Mishra, S.: Limiting DoS attacks during multihop data delivery in wireless sensor networks. Journal of Security and Networks 1(3/4), 167–178 (2006)
8. Liu, D., Ning, P.: Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks. In: Proceedings of 10th annual Network and Distributed System Security Symposium, pp. 263–276 (2003)
9. Perrig, A., Szewczyk, R., Wen, V., Culler, D., Tygar, J.: SPINS: Security Protocols for Sensor Networks. Wireless Networks Journal (WINET) 8(5), 521–534 (2002)
10. Song, H., Zhu, S., Cao, G.: Attack-Resilient Time Synchronization for Wireless Sensor Network. In: Proceedings of IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, vol. (7-7), pp. 772–779 (2005)
11. Dong, J., Ackermann, K.E., Bavar, B., Nita-Rotaru, C.: Mitigating Attacks against Virtual Coordinate Based Routing in Wireless Sensor Networks. In: Proceedings of 1st ACM conference on Wireless Network Security, pp. 89–99 (2008)
12. Soroush, H., Salajegheh, M., Dimitriou, T.: Providing Transparent Security Services to Sensor Networks. In: Proceedings of IEEE International Conference on Communications, pp. 3431–3436 (2007)
13. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy Efficient Communication protocol for Wireless Microsensor Networks. In: Proceedings of the 33rd Hawaii International Conference on System Sciences, vol. 2, pp. 8020–8029 (2000)
14. Zia, T., Zomaya, A.: Security Issues in Wireless Sensor Networks. In: Proceedings of International Conference on Systems and Network Communications, p. 40 (2006)