E-MultiSEC: A New ElGamal based Asymmetric Authentication Technique for WSNs

P. Vijaya Lakshmi[#1], D. Somasundareswari[#2]

[#1]Associate Professor, Hindusthan College of Engineering and Technology
Anna University, Chennai, India.
[#2]Dean, Electrical Sciences, Adithya Institute of Technology
Anna University, Chennai, India.
[#1]vijihicet@gmail.com
[#2]dsomasundareswari@yahoo.co.in

Abstract— **Providing security service in wireless sensor networks using authentication techniques turns out to be a non-trivial task due to network resource constraints. To improve the network security it is often necessary to combine intrusion detection techniques with the key management protocols. Several symmetric key cryptographic solutions proposed earlier are inefficient against node compromise attacks due to complicated key management and delay in the disclosure of secret keys. On the other hand, conventional public key cryptographic techniques have simple and clean key management but suffer from large key size introducing more communication overhead, computational time and delayed authentication. This paper presents E-MultiSEC, a highly reliable authentication technique based on ElGamal signature scheme to provide an efficient secured environment against node compromise attacks in wireless sensor networks. Any compromised node is detected and isolated in the initial stage itself with minimum overheads and energy consumption. The best and fresh route is formed using intermediate nodes between the source and the sink. In addition, this scheme exploits the use of only one ElGamal signature to authenticate the messages which in turn reduces the overhead of the sink in key generation and performing signature verification. A modification of an existing data authentication technique using signatures with hash-chaining is presented, and the modified technique is compared to the original scheme. Simulation results show that our proposed scheme is more advantageous in terms of authentication delay, computation overhead, packet loss, throughput and key generation by sink. The proposed scheme is also more resilient to node compromise attacks and can be applied for different routing techniques in a sensor network.**

Keywords- Authentication, Security, compromised nodes, Wireless Sensor Networks, ElGamal.

I. INTRODUCTION

A Wireless Sensor Network (WSN) in general is a collection of small, low-cost, and low battery powered sensor nodes that communicate with each other through wireless link under highly resource constrained hostile environment. These networks find wide applications in the areas of healthcare, environment monitoring, and military. The growth of WSN applications involving sensitive environments brings the necessity to provide security in the communication traffic between various sensor nodes in the network. Designing security services such as authentication and key management are critical to provide a secure communication between sensor nodes in such hostile environments.While symmetric-key schemes are efficient in processing time for sensor networks, they generally require complicated key management, which may result in large memory and communication overhead. On the contrary, public key based schemes provide simple key management policies, but cost more computational time. Public key schemes have many advantages such as communication overhead, storage, scalability; it can provide simpler solution with much stronger security strength. Several researchers [1-3] have shown that public key schemes are valid on sensor node and the computational cost is expected to fall faster than the cost to transmit and receive.

The rest of the paper is organized as follows. In section 2, the current studies on existing methods are briefly reviewed. Section 3 describes the system model and the methodology involved in implementing the proposed scheme. Section 4 describes the characteristics of E-MultiSEC Technique. In section 5, the experimental results are shown. Finally, a conclusion is given in section 6.

II. RELATED WORKS

Regarding the security issues in the wireless sensor network, the encrypting scheme must not increase the load of sensor nodes. If sensor nodes need to perform complex computations for encryption, it would consume the energy of sensor nodes. Hence, the traditional encrypting and decrypting method is not suitable for wireless sensor networks. Several research surveys were conducted on various public key authentication schemes by Baek in [4] and also on key distribution schemes by Camtepe in [5] for wireless sensor networks. In the public-key based approach, each message is transmitted along with the digital signature of the message generated using the sender's private key. Every intermediate forwarder and the final receiver can authenticate the message using the sender's public key [6-8]. A key requirement for WSN is source node authentication [9]. Remote user authentication schemes were introduced based on source node identity by Das in [10] and also for multicast environments by Leung, etal.in 2003 [11]. Zhang in 2009 [12] proposed techniques for Pre-distribution of keys based on Group re-keying to reduce the number of keys used. Most of the authentication techniques focus on protocol implementations in the network and link layers. Some works based on RSA algorithms that showed optimistic results were addressed by Wander in 2005 [13]. Watro, in 2004 [14] proposed TinyPK authentication scheme which employs RSA and Diffie-Hellman algorithms to calculate an encrypted public key. This protocol is open to hostile attack like spoofing. Later, a less complex, light-weight, dynamic authentication protocol using a hash function and security features of the IEEE 802.15.4 MAC layer was proposed by Wong in 2006 [15]. Perrig and his team in 2000 [16] proposed TESLA, a secure source authentication for multicast had the problem of time synchronization and delayed authentication. Later on the same authors in. 2001 [17] proposed a modification in TESLA which allows receivers to authenticate most packets as soon as they arrive. Several other schemes were also proposed to improve the authentication at the broadcast level by Chang, in 2006 [18] and Ren, in 2007 [19]. Public key authentication schemes applied to WSNs had the drawback of large overhead in terms of computational, communication and storage except for some specific cryptographic applications based on elliptic curve primitives were proposed by Wang in 2006 [20].. Rahman in 2010 proposed a Private Key agreement schemes that proved to be more secure for hetero generous sensor networks. In recent years, the use of pairing-based cryptographic schemes in WSN environments has been proposed for stronger protection. These techniques showed faster response using and smaller sized keys as said by Xiong in 2010 [21]. However, such schemes still have to address the issues of key revoking since the sensor nodes can easily be compromised. Apart from these, authors in [22-25] have suggested several techniques for cross-layer design and energy efficiency.

We propose a novel user authentication technique for wireless sensor networks, using ElGamal signature scheme and a simple hash function to provide high security for a node joining the network and also for the data transmission between the source and the sink. It is assumed that there is only one sink that is endowed with sufficient energy supply. The sink cannot be compromised by any adversaries and it has a secure mechanism to authenticate its messages to all the nodes in the network. We also assume every sensor node has an individual secret key shared with the sink to verify the received messages. Further, there is a unique pair wise key shared between each pair of neighbouring nodes. Contrary to the sink, sensor nodes are resource constrained and are vulnerable to compromised node attacks by adversaries. A reliable transmission mechanism using a link-layer, hop-by-hop acknowledgment protocol is established so that various types of packets in our scheme are not lost.

III. SYSTEM MODEL AND METHOLOGY

A. Threat Model and Assumptions

The wireless sensor networks are assumed to consist of a large number of sensor nodes. We assume that each sensor node knows its relative location in the sensor domain and is capable of communicating with its neighbouring nodes directly using geographic routing. The whole network is fully connected through multi-hop communications. We assume that sink node is responsible for generation, storage and distribution of the security parameters among the network and can never be compromised. However, after deployment, we assume that an adversary can compromise a small fraction of sensor nodes and can gain control on these nodes. Once a sensor node is compromised, it can disrupt the normal operation of the underlying routing protocol by message dropping on purpose, or denial of message attacks to deprive other nodes from receiving messages of the sink. The compromised nodes can be reprogrammed and fully controlled by the attackers. However, the compromised nodes will not be able to create new public keys that can be accepted by the sink and other nodes. One of the limitations of the public key based scheme is the high computational overhead. The recent progress on asymmetric key schemes shows that the public-key schemes can be more advantageous in terms of computational complexity, memory usage, and security resilience, since public-key based approaches have a simple and clean key management [1,2].

This paper considers only active attacks can only be launched from the compromised sensor nodes. Once the sensor nodes are compromised, the adversaries will obtain all the information stored in the compromised nodes, including the security parameters of the compromised nodes. The adversaries can modify the contents of the messages, and inject their own messages. In this paper, we propose an unconditionally secure message authentication scheme E-MultiSEC based on the ElGamal signature scheme on elliptic curves. Our scheme is secure against compromised node attacks and enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power. In addition our scheme provides compromise-resiliency, flexible-time authentication and source identity protection. Simulation results demonstrate that our proposed scheme is more efficient than the basic MultiSEC scheme under comparable security levels.

B. Design Goals

Our proposed authentication scheme aims at achieving the following goals:

• Message authentication: The message receiver should be able to verify whether a received message is sent by the source node that is claimed or by a node in a particular group. In other words, it should be impossible for an adversary to pretend to be an innocent node and inject fake messages into the network without being detected.

• Message integrity: The message receiver should be able to verify whether the message has been modified en-route by the adversaries. In other words, the adversaries should not be able to modify the message content without being detected.

• Hop-by-hop message authentication: Every forwarding node on the routing path should be able to verify the authenticity and integrity of the messages upon reception.

• Identity and location privacy: It should be impossible for an adversary to determine the sender's identity and location by analysing the message contents or the local traffic.

• Node compromise resilience: The scheme should be resilient to node compromise attacks.

• Efficiency: The scheme should be efficient in terms of both computational and communication overhead. It should minimize the cost in computation, communication and storage.

C. An Overview

In this section, we present an overview of the E-MultiSEC scheme, designed to provide high security in a distributed wireless senor network. The sink generates the key pair (PR_{sink}, PU_{sink}); PR_{sink} is the private key and PU_{sink} is the public key of the sink. PU_{sink} is stored by all sensor nodes in the network during node deployment. Similar to the sink, each sensor node S holds a pair of keys (PR_S, PU_S); PU_S is the public key and PR_S is the private key. It is assumed that each source node S is surrounded by a set of neighbours denoted by a vector $N_S = [n_i]_{i=1,\ldots,n}$. Let the data from the source nodes $[S_i]_{i=1,\ldots,m}$ to the sink be denoted by a vector $D = [m_i]_{i=1,\ldots,k}$, in total $k + 1$ data blocks. The data D is partitioned and organized as k blocks. Each data block m_i is regarded as a message authenticating unit. The first block m_0 contains an authenticator, additional information like MAC or signature to authenticate a data block. Each of the other *k-1* blocks also contains a specified authenticator. This paper presents a new authentication scheme based on ElGamal signature scheme and hash function. The following steps are executed to perform an authenticated data transfer from a source node to sink.

Step1. The source node initially broadcasts a route request R_{REQ} to the sink through its next hop neighbours. The R_{REQ} message includes source node's identity ID_S, its public key $PU_{S,}$ and a unique sequence number *SN*, set to 0 initially. *SN* indicates the freshness of R_{REQ} and is incremented for every new R_{REQ} initiated.

Step2. The neighbouring nodes check for the authenticity and freshness of R_{REQ} by looking at the Sequence Number Table (*SNT*).If R_{REQ} is found to be authentic; the request is forwarded to the next neighbour. Otherwise, the source node is registered as a compromised node. Each neighbouring node in the forward path checks for the authenticity and freshness of R_{REQ} and forwards the request to the sink.

Step3. Sink verifies for the validity of PU_S and generates a Certificate $C_{S.}$

Step4. Sink signs the Certificate C_S using its private key PR_{sink} and sends *Cs* to authenticate the source node that has send the R_{REQ}. *Cs* is of the form shown below.

$$C_S = ID_C \| ID_S \| PU_S \| SN,\ SIG_{PRsink}\{h(ID_C \| ID_S \| PU_S \| SN)\}$$

Step5. The source node computes hash values of all data blocks, obtains the message digest as

$\mathcal{D} = H\ (CON(D))$ where $CON(D) = d_1 \| d_2 \| \ldots \| d_k$.

Source Node S generates a signature for the data to transmit using hash function as

$$SIG_{PRsink} = \mathcal{D} \| \mathcal{E}(PR_s, \mathcal{D}).$$

The source node sends the signature and the data along with the C_S to the sink of the form $[SIG_{PRsink}, C_S]$

Step6. Sink checks for the data authenticity through verification.

If $\mathcal{D}(PU_S, \mathcal{E}(PR_S, \mathcal{D})) = \mathcal{D}$, *then* $\mathcal{D}$ is said to be authentic.

The sequence of steps involved is shown in Fig. 1.

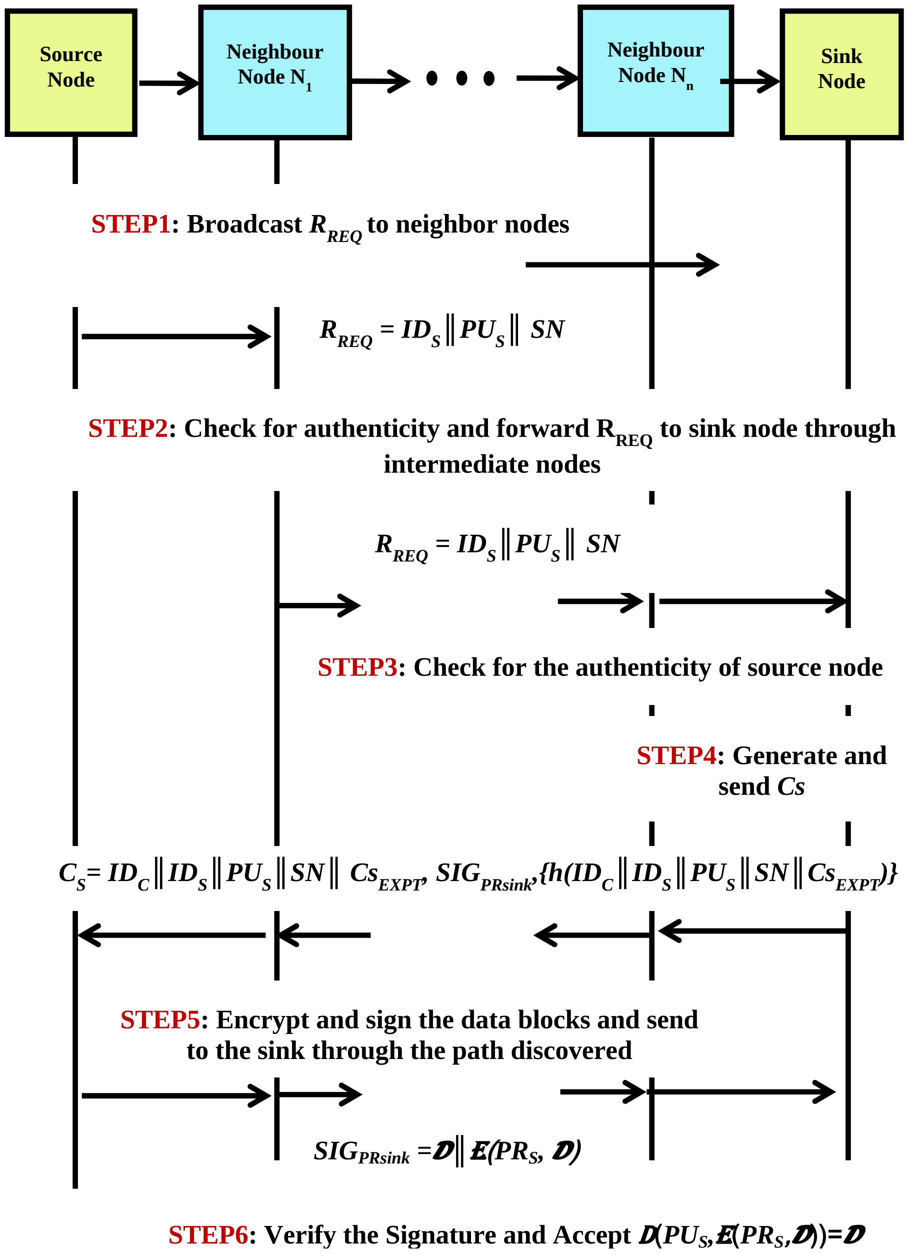
Source Node
Neighbour Node N1
Neighbour Node Nn
Sink Node
STEP1: Broadcast R_{REQ} to neighbor nodes
$R_{REQ} = ID_S \| PU_S \| SN$
STEP2: Check for authenticity and forward R_{REQ} to sink node through intermediate nodes
$R_{REQ} = ID_S \| PU_S \| SN$
STEP3: Check for the authenticity of source node
STEP4: Generate and send Cs
$C_S = ID_C \| ID_S \| PU_S \| SN \| Cs_{EXPT}, SIG_{PRsink}, \{h(ID_C \| ID_S \| PU_S \| SN \| Cs_{EXPT})\}$
STEP5: Encrypt and sign the data blocks and send to the sink through the path discovered
$SIG_{PRsink} = D \| E(PR_S, D)$
STEP6: Verify the Signature and Accept $D(PU_S, E(PR_S, D)) = D$

Fig. 1 Step by Step Procedure describing E-MultiSEC Authentication Technique

IV. PROPOSED SCHEME

We propose a novel PKC based authentication scheme for WSNs to meet the following properties.

- Reduced computation and communication overhead; almost same as that of HMAC.
- It is very difficult for an adversary to compromise the sink to launch a valid authentication.
- Use of ElGamal to sign the first block message itself provides the necessary authenticity to the receiver.
- More resilience to node compromise attacks.

A. Sensor Nodes Initialization and Deployment

The *sink* first chooses p to be a large prime and q a generator of Z_p*. Then, the *sink* selects a secure cryptographic hash function *h( )*, where $h : \{0, 1\}^* \longrightarrow Z_p^*$. Finally, the *sink* sets the public parameters as *params*= $\{p, q, h( )\}$. To initialize sensor nodes $S = \{S_0, S_1, S_2, \cdot \cdot \cdot\}$, the *sink* invokes the Algorithm 1. Then, the *sink* deploys these initialized sensor nodes at a certain region through various ways by air or by land. We assume that all sensor nodes are randomly distributed after deployment.

Algorithm 1 Network Initialization Algorithm

```
Procedure Network Initialization
Input: params = {p, q, h( )} and Uninitialized Network S={$S_i$}, i=1,2,3,4…n
Output: Network Initialized
for each sensor node $S_i$    S, do
    preload $S_i$ with parameters T = (p, q, h) and initial energy.
    compute the public key $PU_S$ and private key $PR_S$ and install in $S_i$
end for
return Network Initialization
end procedure
```

B. Route Discovery and Certificate Generation

A sensor node that has some data ready to transmit performs the following steps to discover the route from the source node to the sink. The source node broadcasts a route request R_{REQ} to all its 1-hop neighbour nodes as shown below in Fig.2.

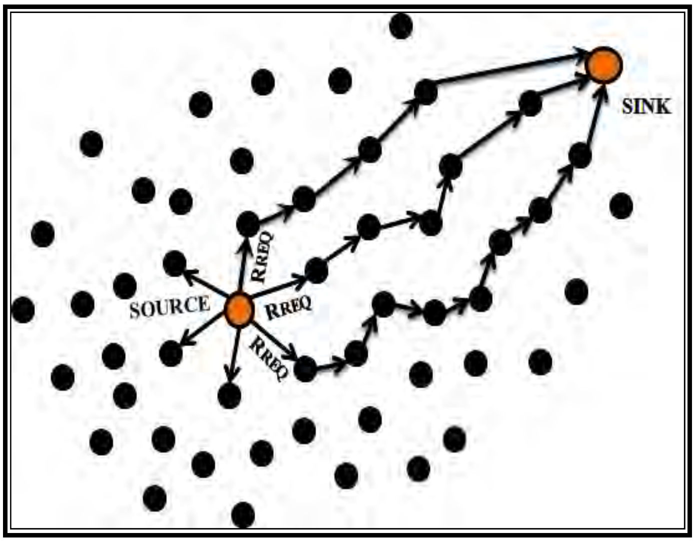

Fig.2 Route request

The neighbouring nodes check for the authenticity and freshness of the R_{REQ} by looking at the Sequence Number Table (*SNT*).R_{REQ} includes source node's identity ID_S, its public key $PU_{S,}$ and a unique sequence number (*SN*) which is set to 0 initially. *SNT* stores all the above three entries (i.e. ID_S,PU_S,SN) and broadcasts it's identity *B* that uniquely identifies a R_{REQ} in the network. If an entry not equal to '0' is present in the *SNT* for the received R_{REQ}, it is considered as a duplicate and is discarded without further broadcasting. Otherwise, the intermediate node increments the sequence number and updates its routing table for forward path before broadcasting the R_{REQ} message. The neighbour nodes thus create a secured route from source to the sink. Using this route discovery procedure all the available routes between the source and the sink are identified and are stored in the routing table maintained by each node in the network. Before forwarding the R_{REQ} each intermediate node checks for the authenticity of R_{REQ}. Otherwise, it registers the node as a compromised node. The sink generates a certificate C_S for the first fresh R_{REQ} message received and sends this certificate as the response R_{REP} as shown in Fig. 3.

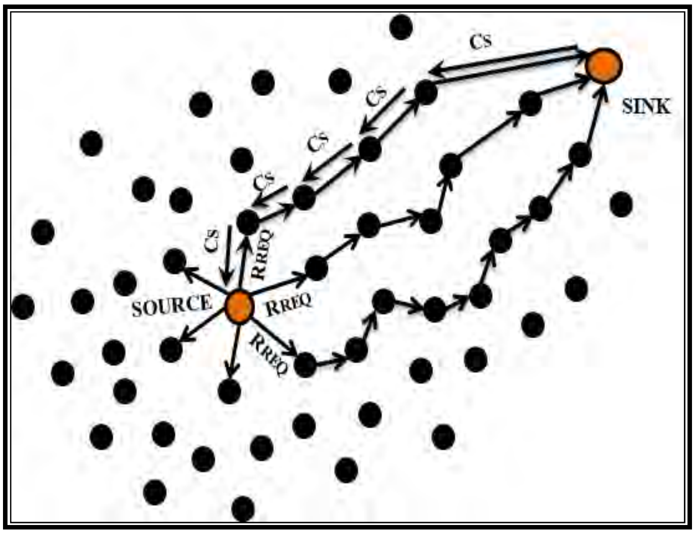

Fig.3 Route discoveries for Certificate Generation

The intermediate nodes are forbidden to send R_{REP} even if they have an active route to sink. The source node transmits the encrypted signed data as soon as it gets R_{REP} through this *main route* to the sink as shown below in Fig. 4. All the other routes that are discovered will be stored in the routing table as *alternate routes*.

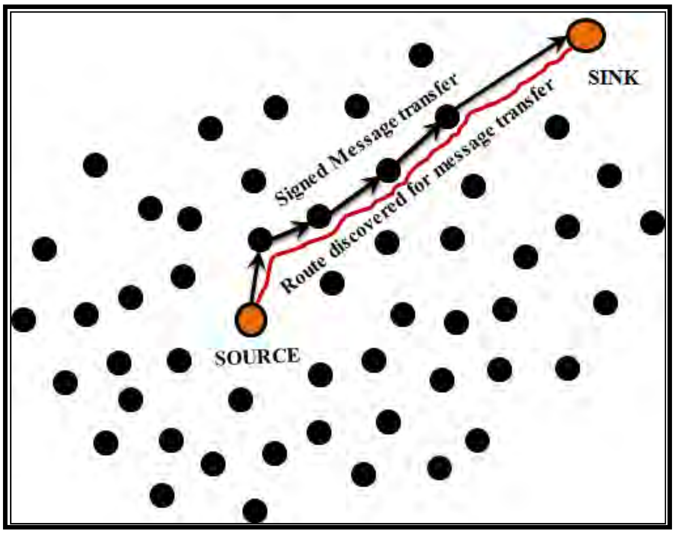

Fig.4 Signed message transmission

The route selection process is such that whenever a route is required for data transmission, it always selects the main route if it is available. If the *main route* is not active, then the route with lowest hop count from the available *alternate routes* is selected. Whenever there is no route available in the routing table, the route discovery process is initiated again and another set of routes are stored. Algorithm 2 shows the sequence of steps involved in route formation and data transmission.

Algorithm 2 Route Formation and Data Transmission

```
1: Procedure Route Formation and Data Transmission
Input: $R_{REQ} = ID_S \| PU_S \| SN$
Output: $R_{REP} = C_S = ID_C \| ID_S \| PU_S \| SN \| E(PR_{sink}, ID_C \| ID_S \| PU_S \| SN)$
2: Broadcast $R_{REQ}$ to each neighbor node $N_{i,}$ i=1,2,3…n
3:          if SN = 0          # Check for the freshness in the entry of the seen table (SNT) #
4:          then Forward $R_{REQ}$.
5:          Else SN = SN+1
6:   Forward $R_{REQ}$          # Increment the entry in the SNT and forward the $R_{REQ}$ #
7:          end if
8:          If $N_i$ = sink
```

```
9:          then Generate $C_S$, Sign $C_S$ and send $R_{REP}$
10:         Else Go to Step 5
11:     end if
12: Select the Main Route
13: Perform data transfer
14: return Route Formation and Data Transmission
15: end procedure
```

C. Message Authentication

In resource constrained environments like wireless sensor networks it is necessary to provide efficient authentication mechanisms to have an effective control on attacks like eavesdropping, node compromise and DoS etc., during which, an adversary is able to intercept messages, change the intercepted messages and retransmit them. Sometimes, the adversary may fabricate messages and inject them to the network that may result in heavy traffic causing destruction of the entire network. The proposed E-MultiSEC uses one ElGamal signature to authenticate all the transmitted messages. The optimal ElGamal signature scheme [17] consists of the three steps as given in Algorithm 3. This in turn reduces the risk in overheads to be controlled by the sink.

Algorithm 3 Optimal Elgamal Signature Scheme

Key generation: Let p be a large prime number and q be a generator of Z_p*. Both p and q are made public. For a random private key x Z_p, the public key y is computed from

$y = g^x \bmod p$.

Signature generation: The algorithm can also have many variants [18], [19]. To sign a message **m**, one chooses a random k Z_{p-1}*, then computes the exponentiation

$r = g^k \bmod p$ and solves s from: $s = rxh(m, r) + k \bmod (p - 1)$where h is a one-way hash function. The signature of message m is defined as the pair (r, s).

Verification: The sink checks the signature equation $g^s = ry^{rh(m,r)} \bmod p$. If the equality holds true, then the verifier accepts the signature, and rejects otherwise.

In E-MultiSEC only one signature is used to authenticate the authenticator in D_0. The authenticator in D_0 is used to authenticate D_1. This process continues until D_k. Authenticators for data blocks are generated using collision resistant hash functions using optimal ElGamal Signature Scheme as given in Algorithm 4.

Algorithm 4: Generation of Signed Data

```
Procedure; Generation of Signed Data
Input: Data $D$, a string of random characters
Output: Signed Data $SIG_{PRsink}=\{\mathcal{D} \| E\ (PRs, \mathcal{D})\}$
1: Partition $D$ into $k$ blocks $d_1, . . .,d_k$, $D=[d_i]^T_{i=1,2,..,k}$
2: Initialize $d$ with a string of random characters
3:          for $i= 1$ to $k$; do
4:          Concatenate the data blocks $d_i$ to generate $CON\ (D) = d_1 \| d_2 \| \ldots \| d_k$
5:          Compute Digest $\mathcal{D}$
            $\mathcal{D} = H\ (CON\ (D))$ with a collision resistant hash
6:      end for
7: Generate $SIG_{PRsink} = \mathcal{D} \| \mathbb{E}(PR_s, \mathcal{D})$.
8: return Generation of Signed Data
9: end procedure
```

D. Transmitting Signed Messages

Source node S sends the data D and the certificate C_S to the sink. On receiving the data, the neighbour nodes checks whether D belongs to current source node. If D belongs to S_i, the receiver tries authenticating S_i and D. After authentication of S_i, D will be transmitted to the next node along the route after a short back-off. This process continues until the message reaches the sink.

E. Verifying Extended Blocks

According to the algorithm, *SM* is authenticated by the signature, that is, if the decryption $\mathbb{D}(PU_S,\mathbb{E}(PR_S,\mathcal{D})) =\mathcal{D}$, *then* $\mathcal{D}$ is said to be authentic.

V. PERFORMANCE ANALYSIS

In this section we first analyse the security aspects of the proposed E-MultiSEC protocol. We then analyse the overheads in computation, communication, authentication delay, and packet loss of the proposed scheme with the basic scheme. Our analysis is based on a randomly, uniformly deployed sensor network with 150 nodes. On average, each sensor has 10 neighbours. The senor nodes IDs have the size of 2 bytes. The random keys have the size of 10 bytes. With additional 2 bytes for key indices, each pre-distributed random key requires 12 bytes for memory space.

A. Security

As the proposed scheme is based on asymmetric key cryptography, it is inherently more resilient to node compromise attacks. Authentication sensitive information like PU_{sink}, PU_S and the digest will be known to an adversary only if the sink is compromised. However, the adversary can neither create a valid certificate using PU_{sink}, nor generate the signature for d_0 with PU_s. *H* being collision resistant hash an adversary cannot forge d_i using the digest $\boldsymbol{D}$or impersonate a valid source node even after compromising it. In the proposed technique, an optimal ElGamal signature scheme is used to authenticate d_0 while the remaining *k-1* data blocks are authenticated by the digest of the previous data blocks. Thus, the authentication of d_i is equivalent to the authentication by an ElGamal signature. Also, we see that d_i is the input to compute d_i in $d_{i-1,}$ d_{i-1} is the input to compute d_{i-1} in d_{i-2} and finally, d_1 is the input to compute d_1 in d_0. Use of collision resistant hash makes it is computationally infeasible for an adversary to forge D_i without changing d_1.

B. Overhead

In our sensor network, to minimize the communication and computation overhead we aim is to find the optimum local connectivity that will provide maximum resilience against compromised nodes.

The average time required to authenticate one data block in *D* at the source side is $\boldsymbol{T_{source}}$ as shown in equation (1).

$$\boldsymbol{T_{source}} = \frac{\boldsymbol{T_{sign} + k\, T_{hash}}}{\boldsymbol{m}} \qquad \text{---------- (1)}$$

The average time to authenticate one broadcast message at the sink side is $\boldsymbol{T_{sink}}$ is given in equation (2).

$$\boldsymbol{T_{sink}} = \frac{\boldsymbol{T_{verify} + k\, T_{hash}}}{\boldsymbol{m}} \qquad \text{---------- (2)}$$

The communication overhead is determined by the message length. The large communication overhead of the basic scheme will increase the energy consumption and authentication delay. The simulation results in Fig. 5 demonstrate that our proposed scheme has much lower energy consumption and hence less authentication delay.

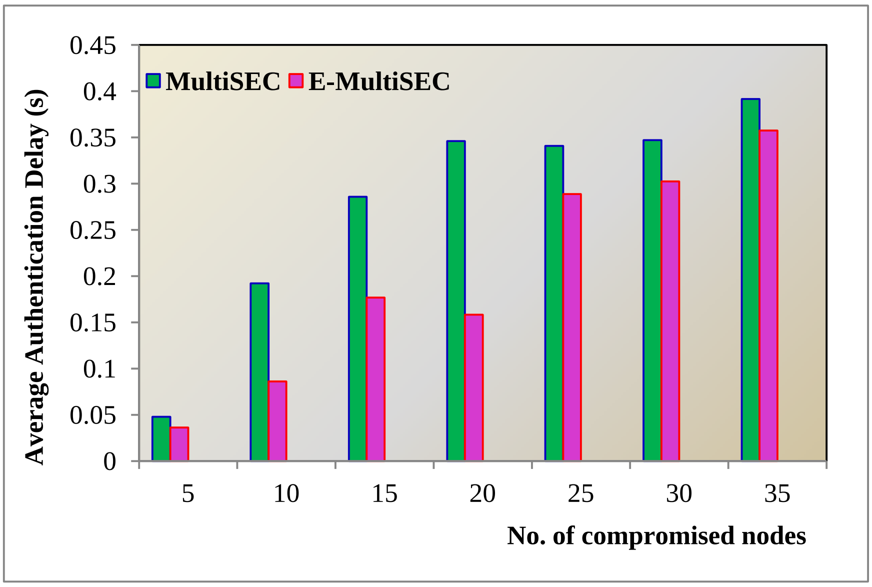

Fig. 5 Relation between Authentication delay and compromised nodes

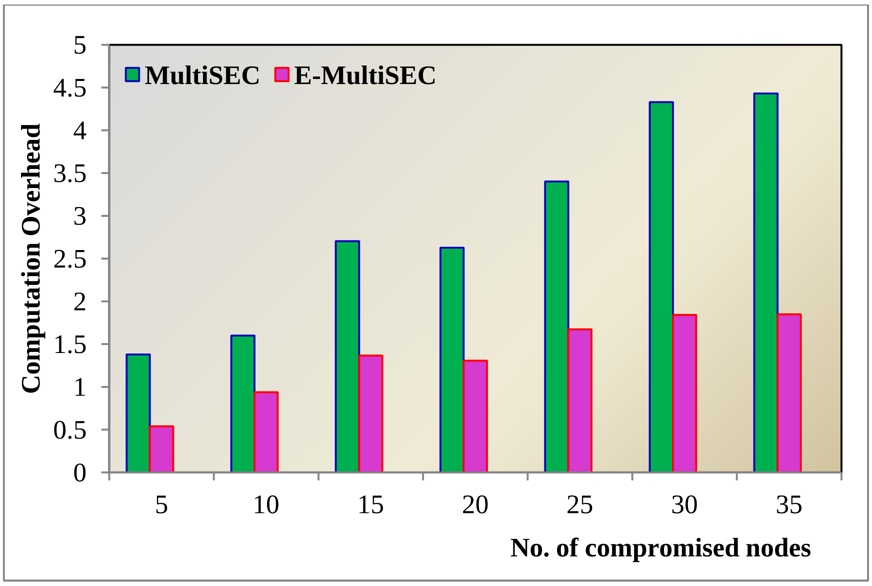

Fig.6 Relation between Computation Overhead and compromised nodes

TABLE I
Performance Comparison of Authentication Delay and Computation Overhead

No. of compromised nodes	Authentication Delay		Computation Overhead	
	MultiSEC	E-MultiSEC	MultiSEC	E-MultiSEC
5	0.047974	0.036252	1.380	0.540
10	0.192121	0.086209	1.600	0.938
15	0.285809	0.158344	2.704	1.306
20	0.340793	0.176770	3.402	1.366
25	0.345958	0.288650	2.628	1.672
30	0.346962	0.302309	4.330	1.842
35	0.391551	0.357406	4.430	1.848

The communication overhead is determined by the message length. The large communication overhead of the basic scheme will increase the energy consumption and authentication delay. The simulation results shown in TABLE I demonstrate that our proposed scheme has much lower energy consumption and hence less authentication delay.

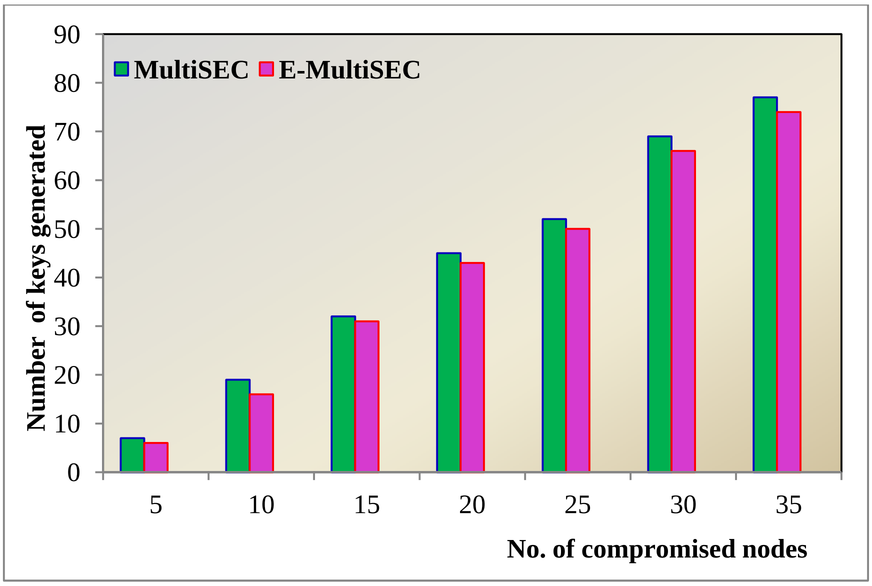

Fig.7. Relation between keys generated and compromised nodes

Fig.7 shows the relation between the number of keys generated by the sink node to the increase in the number of compromised nodes. There is considerable reduction in the number of keys generated by the sink node towards the increase in the percentage of compromised nodes. This shows an improvement in the network performance.

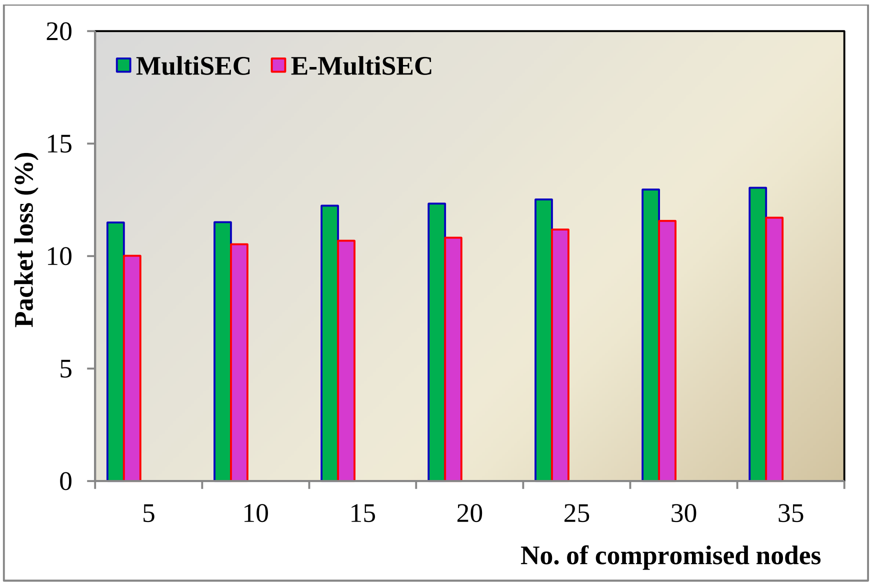

Fig. 8 Packet Loss Characteristics

As shown in Fig. 8, the packet loss experienced in E-MultiSEC is also comparably very less to that of the basic protocol. Fig. 9 shows a large improvement in throughput when compared to MultiSEC, the basic secret key protocol for WSN. Finally, it is observed that proposed scheme is as secure as conventional PKC based authentication scheme.

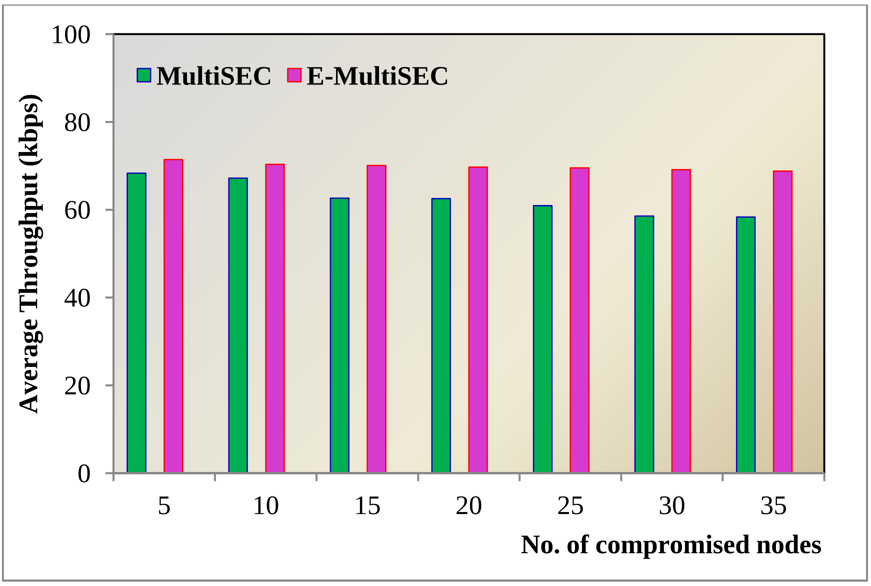

Fig. 9Average Throughput

The simulation results shown in TABLE II demonstrate that our proposed scheme has much lower number of keys generated. This in turn reduces the burden on the sink and also the overall communication overhead. Reduction in communication overhead has a direct impact on the packet loss and throughput. Decrease in packet loss has improved the throughput of the network.

TABLE II
Performance Comparison of Packet loss, No. of keys generated by the sink and Average Throughput

No. of compromised nodes	No. of keys generated by the sink		Packet Loss (%)		Average Throughput (kbps)	
	MultiSEC	E-MultiSEC	MultiSEC	E-MultiSEC	MultiSEC	E-MultiSEC
5	7	6	11.49026	10.01294	68.350	71.420
10	19	16	11.50564	10.52268	67.204	70.342
15	32	31	12.23490	10.68087	62.658	70.100
20	45	43	12.32610	10.81596	62.536	69.714
25	52	50	12.51192	11.17924	60.924	69.538
30	69	66	12.95286	11.56280	58.550	69.120
35	77	74	13.03230	11.70120	58.330	68.796

VI. Conclusion

Design of security techniques for WSNs requires more efficient methods to perform mutual authentication in an insecure network environment. In this paper, we have proposed an efficient authentication scheme based on ElGamal together with compromised node detection to provide a mutual authentication between any pair of sensor nodes in a wireless sensor network. The proposed protocol can also protect inside security and outside security. Furthermore, it not only inherits the merits of ElGamal-based mechanism but also enhances the WSN authentication with higher security than other protocols. Therefore, the proposed protocol is more suited to WSNs environments. Our protocol has the following features: It is suitable for both static and dynamic WSNs. The system is scalable and resilient against node compromise. In comparison with the basic protocol, our protocol could save about 30% in communication with less delay and cost than those pre-distribution schemes, without incurring in a considerable amount of communication.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their careful reading; insightful comments and suggestions that have helped us improve the presentation of this paper.

REFERENCES

[1] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz, “Energy analysis of public-key cryptography on small wireless devices,” IEEE International Conference on Pervasive Computing and Communications (PerCom'05), pp. 324–328, 2005.

[2] H. Wang, S. Sheng, C. Tan, and Q. Li, “Comparing symmetric-key and public-key based security schemes in sensor networks: A case study of user access control,” in *IEEE ICDCS*, Beijing, China, pp. 11–18, 2008.

[3] W. Du, R. Wang, and P. Ning, “An Efficient Scheme for Authenticating Public Keys in Sensor Networks,” In *Proceeding of the MobiHoc*, pp.58– 67, 2005.

[4] J. Baek, H. C. Tan, J. Zhou, and J. W. Wong, “Realizing Stateful Public Key Encryption in Wireless Sensor Network”, *IFIP- The International Federation for Information Processing*, Volume 278, pp. 95-107, 2008.

[5] S.A. Camtepe, and B.U. Yener, “Key Distribution Mechanisms for Wireless Sensor Networks: A Survey”, *Technical Report TR-05-07; Department of Computer Science, Rensselaer Polytechnic Institute*: Troy, NY, USA, 2005.

[6] R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the Assoc. of Comp. Mach*., vol. 21, no. 2, pp. 120–126, 1978.

[7] D. Pointcheval and J. Stern, “Security arguments for digital signatures and blind signatures,” Journal of Cryptology, vol. 13, no. 3, pp. 361–396, 2000.

[8] T. A. ElGamal, “A public-key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472,1985 .

[9] I.F.Akyildiz, W. Su, Y. Sankarasubramaniam, and E.Cayirci, “Wireless Sensor Networks: A Survey”, *Journal of Computer Networks,* vol. 38, pp. 393-422, 2002.

[10] M.L. Das, A. Saxena, and V.P. Gulati, “A Dynamic Id-Based Remote User Authentication Scheme”, *IEEE Transactions on Consumer Electronics, v*ol.50, pp. 629-631, 2004.

[11] K.C. Leung, L.M. Cheng, A.S. Fong and C. Chan, “Cryptanalysis of a Modified Remote User Authentication Scheme Using Smart Cards”, *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1243-1245, 2003.

[12] W. Zhang, S. Zhu, and G. Cao, “Predistribution and Local Collaboration-Based Group Rekeying for Wireless Sensor Networks”, *Journal of Ad Hoc Networks*, vol.7, pp. 1229-1242, 2009.

[13] R.J. Watro, D. Kong, S.F. Cuti, Ch. Gardiner, Ch. Lynn, and P. Kruus, “TinyPK: Securing Sensor Networks with Public Key Technology”,*In Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, USA, pp. 59-64, 2004.

[14] K.H.M. Wong, Y. Zheng; J.Cao; S.Wang, “A Dynamic User Authentication Scheme for Wireless Sensor Networks”, *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Taiwan*, vol.1, no. 8, pp. 986 – 990, 2006.

[15] Perrig, R. Canetti, D. Song, J. D. Tygar, “Efficient and Secure Source Authentication for Multicast”, *Proceedings of the Internet Society Network and Distributed System Security Symposium (NDSS 2001)*, pp. 35-46, 2001.

[16] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar, “SPINS: Security Protocols for Sensor Networks”, *MOBICOM*,, pp. 189-199,2001.

[17] S.M. Chang, S. Shieh, W.W.Lin, C.Hsieh, “An efficient Broadcast Authentication Scheme in Wireless Sensor Networks”, *Proceedings of ACM Symposium on Information, Computer and Communications Security, Alexandria, VA, USA,* pp. 311-320, 2006.

[18] K. Ren, W.Lou, K. Zeng, P.J. Moran, “On Broadcast Authentication in Wireless Sensor Networks”, *IEEE Transactions on Wireless Communications*, vol.6, pp. 502-514, 2007.

[19] H. Wang, and Q. Li, “Efficient Implementation of Public Key Cryptosystems on Mote Sensors”, *Information and Communication Security, Lecture Notes in Computer Science*, vol. 4307, pp. 519–528, 2006.

[20] S.M.M. Rahman, and K. El-Khatib, “Private Key Agreement and Secure Communication for Heterogeneous Sensor Networks”, *Journal of Parallel and Distributed Computing*, vol.70, no.8, pp. 858–870, 2010.

[21] X. Xiong, D.S. Wong and X. Deng, “Tiny Pairing: a Fast and Lightweight Pairing-Based Cryptographic Library for Wireless Sensor Networks”, *IEEE Wireless Communications and Networking Conference (IEEE WCNC10)*, Sydney, Australia, 2010.

[22] S. Li, X. Ma, X. Wang and M. Tan, “Energy efficient multipath routing in wireless sensor network considering wireless interference”, *Journal of Control Theory Applications*, vol. 9, pp. 127-132, 2011.

[23] M. Tabibzadeh, M. Sarram , and F. Adibnia, “Hybrid Routing Protocol for Prolonged network Lifetime in Large Scale Wireless Sensor Network”, *Proceedings of International Conference on Information and Multimedia Technology*, pp.179-183, 2009.

[24] Zhang and A. Seyedi, “Analysis and design of energy harvesting wireless sensor networks with linear topology”, *Proceedings of IEEE ICC*, pp.1-5, 2011.

[25] K. Babulal and R. Tewari, "Cross Layer Design for Cooperative Transmission in Wireless Sensor Networks," *Wireless Sensor Network*, vol. 3, pp. 209-214, 2011.

BIOGRAPHY

P.Vijaya Lakshmi is working as Associate Professor in the Department of Electronics and Communication Engineering at Hindusthan College of Engineering and Technology, Coimbatore, India. She holds a Masters Degree in VLSI Design from Anna University, Chennai and Bachelors degree in Electronics and Communication Engineering from Bharathiyar University, Coimbatore. She has more than 17 years of teaching experience. She has organized several workshops, conferences and published papers in national and international journals and conferences. She also leads and teaches modules at both B.E and M.E levels in Electronics and Communication Engineering. Her research interest includes Wireless Communications and VLSI Design.

D.Somasundareswari is working as Dean, Electrical Sciences at Adithya Institute of Technology, Coimbatore, India. She holds a B.E. Degree in Electrical and Electronics Engineering and M.E., Degree in Electrical Machines and Ph.D. Degree from Anna University, Chennai. She has more than 21 years of teaching experience. She is a life member of ISTE, SSI and member of IE. She has published more than 45 research papers in the National and inter-national Journals and Conferences. Her research interest includes Soft Computing, Electrical machines, Digital Image Processing and VLSI Design.