VOL. 10, NO. 14, AUGUST 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

SOURCE AND DESTINATION ANONYMITY USING END-TO-END ANONYMOUS ADDRESSING SCHEME IN WSN

D. Angeline Deborah Monica[1], S. Karthikeyan[2]and V. Brindini[1]
[1]Electronics and Communication Engineering Sathyabama University, Tamil Nadu, Chennai, India
[2]Faculty of Electrical and Electronics,Sathyabama University, Tamil Nadu, Chennai, India
E-Mail: angeline7893@gmail.com

ABSTRACT

The wireless sensor network is most widely used for the critical applications; we need to provide the anonymity for the source and destination. The proposed scheme named as End to End anonymous addressing scheme will provide anonymity with less computational and storage overhead. In the proposed scheme, the hop by hop authentication is provided by using the Elliptic Curve Cryptography (ECC) based Digital signature scheme. The source node sends the message along with signature. Each and every intermediate node should validate the signature to ensure that it receives the message from authenticated node. It will forward to next hop node, only the signature is valid otherwise it will drop the message. The anonymous address scheme is used to provide the destination anonymity. In this technique, the Duplicate Address List (DAL) is constructed by destination and send to the source node. The source node attaches this DAL with DATA packet. To provide high security for the destination address the destination address is encrypted by using ECC and then append with DAL. The performance of the proposed scheme is evaluated by using the network simulator NS2. The packet delivery ratio, packet loss ratio, End to End delay is used to evaluate the performance.

Keywords: WSN, elliptical curve cryptography, anonymity, storage overhead, authentication.

1. INTRODUCTION

The wireless sensor network consists of two kinds of node. They are sensor node and base station. The sensor node is a tiny in size and it has very limited amount if battery power for its operation. It is used to sense or monitor the environmental condition like pressure, temperature, humility etc. The Base station is located far away from the sensor nodes. The energy of the base station is not restricted one. The sensor node work cooperatively and collect the monitored data and send it to the base station. The base station process the data collected from the sensor and provide information to the user.

The wireless sensor networks are getting more popular because of its use in the battle field for national security. Nowadays the wireless sensor networks are used in many range of application such as environmental monitoring, forest fire detection system and in many other fields.

The sensor nodes are typically having battery which is replenished one. They are having very limited amount of storage, computational capability and communication ability. As the WSN is widely used in the critical application, the energy conservation [6] of the sensor node should be optimized. The lifetime is a very acute parameter in wireless sensor network.

The proposed technique reduces transmission delay by using opportunistic routing and also the trust value is calculated by using the additional parameter link quality. It ensures reliability and provide high system throughput.

The recent technological advances make wireless sensor networks (WSNs) technically and economically feasible to be widely used in both military and civilian applications, such as monitoring of ambient conditions related to the environment, precious species and critical infrastructures. A key feature of such networks is that each network consists of a large number of undeterred and unattended sensor nodes. Awireless sensor network (WSN) consists of hundreds or thousands of sensor nodes and a small number of data collection devices. The sensor nodes have the form of low-cost, low-power, small-size devices, and are designed to carry out a range of sensing applications, including environmental monitoring, military surveillance, fire detection, animal tracking, and so on. The sensor nodes gather the information of interest locally and then forward the sensed information over a wireless medium to a remote data collection device (sink), where it is fused and analyzed in order to determine the global status of the sensed area.

Message authentication plays a key role in thwarting unauthorized and corrupted messages from being forwarded in networks to save the precious sensor energy. For this reason, many authentication schemes have been proposed in literature to provide message authenticity and integrity verification for wireless sensor networks. The symmetric-key based approach [7] requires complex key management, lacks of scalability, and is not resilient to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. The shared key is used by the sender to generate a message authentication code (MAC) for each transmitted

message. However, for this method, the authenticity and integrity of the message can only be verified by the node with the shared secret key, which is generally shared by a group of sensor nodes. An intruder can compromise the key by capturing a single sensor node. In addition, this method does not work in multicast networks.

In this paper, we propose a novel anonymous addressing scheme which has been designed for the following objectives.

- To hide node identities and/or routes from outside observers in order to provide anonymity protection.
- To offer high anonymity protection at a low cost

The source and destination anonymity is provided for the Wireless Sensor Networks with low cost using our proposed scheme.

2. RELATED WORKS

This section presents the existing work on providing security for wireless sensor networks.

A. Statistical en-route filtering (SEF)

Statistical En-route Filtering (SEF) requires that each sensing report be validated by multiple keyed message authentication codes (MACs), each generated by a node that detects the same event. The sink further filters out remaining false reports that escape the en-route filtering. SEF exploits [1] the network scale to determine the truthfulness of each report through collective decision-making by multiple detecting nodes and collective false-report-detection by multiple forwarding nodes.

B. Symmetric-key and public-key based security schemes

They have designed a suite of ECC-based access control protocols [2] including pairwise key sharing between neighboring sensors, local access control, and remote access control. They believe the integral security application sheds new insights into the practicality of the PKC based scheme in sensor networks, and provides a deeper understanding of the security protocol design in a resource constrained system.

They have provided a detailed comparison of symmetric cryptography and PKC based user access control Protocols. This paper builds the user access control on commercial off-the-shelf sensor devices as a case study to show that the public-key scheme can be more advantageous in terms of the memory usage, message complexity, and security resilience.

C. Resilient message authentication

A novel message authentication approach which adopts a perturbed polynomial-based technique to simultaneously accomplish the goals of lightweight, resilience to a large number of node compromises, immediate authentication, scalability, and non-repudiation.

In [3], they propose a new message authentication approach to address the high communication or computation overhead, delayed authentication and lack of scalability. Their approach has following features: lightweight in terms of computation, communication and storage overhead; resilience to a large number of sensor node compromises; immediate authentication (therefore supporting both synchronous and asynchronous communication); scalability; and non-repudiation.

D. How to leak a secret

Ring signatures provide an elegant way to leak authoritative secrets in an anonymous way, to sign casual email in a way which can only be verified by its intended recipient, and to solve other problems in multiparty computations. The main contribution [4] is a new construction of such signatures which is unconditionally signer-ambiguous, provably secure in the random oracle model, and exceptionally efficient: adding each ring member increases the cost of signing or verifying by a single modular multiplication and a single symmetric encryption.

E. Hop-by-hop authentication scheme

An interleaved hop-by-hop authentication scheme that guarantees that the base station will detect any injected false data packets when no more than a certain number t nodes are compromised.

It provides an upper bound B for the number of hops that a false data packet could be forwarded before it is detected and dropped, given that there are up to t colluding compromised nodes.

In [5], they present a scheme for addressing this form of attack, which we call a false data injection attack. That scheme enables the base station to verify the authenticity of a report that it has received as long as the number of compromised sensor nodes does not exceed a certain threshold. Further, their proposed scheme attempts to filter out false data packets injected into the network by compromised nodes before they reach the base station, thus saving the energy for relaying them.

3. PROPOSED METHOD

A. Source and destination anonymity

As the wireless sensor is most widely used for the critical applications, we need to provide the anonymity for the source and destination. The proposed scheme named as End to End anonymous addressing scheme will provide anonymity with less computational and storage overhead.

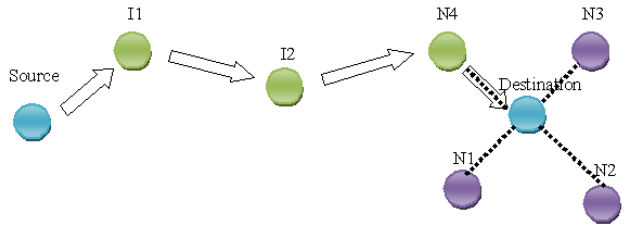

Figure-1. Source and destination annonymity by end to end addressing scheme.

In the proposed scheme, the hop by hop authentication is provided by using the Elliptic Curve Cryptography based Digital signature scheme. The source node sends the message along with signature. Each and every intermediate node should validate the signature to ensure that it receives the message from authenticated node. It will forward to next hop node, only the signature is valid otherwise it will drop the message.

The proposed scheme follows following steps to provide end to end anonymity in the Wireless Sensor Networks.

- Initially, the source node sends the RTS (Request to Send) message to Destination node to know its availability.
- If it is available, it will reply with CTS (Clear to Send) message along with its duplicate address.
- The destination node frames its duplicate address in the following way:
- The destination node adds the ID of all the nodes available in its neighbor list into the address frame, at last add its identity which is encrypted by using ECC. The destination node shares its key with all its neighbors. So, the neighbor can only know the address of the destination.
- For the network mentioned by the above Figure-1, the duplicate address will be,

N1	N2	N3	N4	D

- After receiving CTS from destination node, the source node sends the data with signature, route (Intermediate node IDs) and duplicate address list received along with the CTS message.
- All the intermediate nodes check for authentication of the sender node as well as check its presence in the address list. If the Id of the any intermediate node is present in the address list, it should be a neighbor node of the destination and also it should have the key to decrypt the address of the destination. It will take the last address in the list as the destination address and get the original Id by using the key.
- After that, forward the message to the actual destination node.

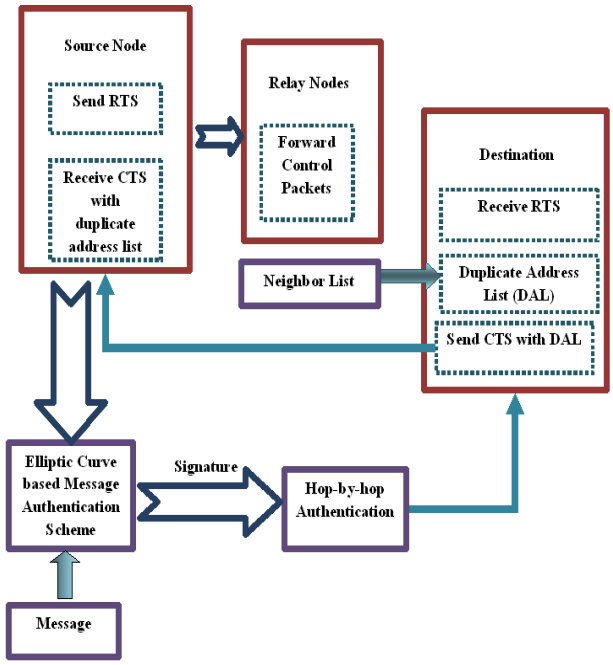

Figure-2. Block diagram of the proposed scheme

The Figure-2 presents the overall process of our proposed scheme. In our research work, we consider the multihop communication of sensor network. Generally, if the sensor present inside the communication range of the Sink or Bases station in the sense, it can directly transmit the data else it will transmit through some intermediate nodes. The second case is called as multihop communication. The intermediate nodes are otherwise called as relay nodes. The source sensor node sends the RTS packet to the destination node through relay nodes. After receiving RTS, the destination compute its duplicate address list and then it will send back the CTS with this duplicate address list.

The message to be transmitted is signed by using Elliptic curve based Message authentication scheme. Each and every relay node verifies this signature to ensure Hop by Hop message authentication. The Algorithm1 explains the source and destination anonymity by using anonymous addressing scheme.

B. Anonymous addressing scheme

Algorithm1

1. *Dn →Destination address*
2. *Sn →Source Address*
3. *NL →Neighbor List*
4. *Set dal →ϕ*
5. *Function Duplicate address list (Dn, NL) {*

6. *For each neighbor node in NL {*
7. *N_addr→Neighbor node address*
8. *Append dal N_addr*
9. *}*
10. *E_D_Addr→Encrypted Destination Address #Using ECC Algorithm*
11. *For each neighbor node in NL*
12. *Broadcast its secret key to all node in NL*
13. *Append dal E_D_Addr*
14. *Return dal*
15. *}*
16. *Soc→Sn*
17. *Route →ϕ ϕ*
18. *Relay_node→sn*
19. *Function Shortest Path (Sn, Dn) {*
20. *For each node in NL (soc) {*
21. *If {$Dn==$neighbornode} {*
22. *Relay_node→Dn*
23. *}*
24. *}*
25. *While (Relay_node!=Dn) {*
26. *For each node in NL (soc) {*
27. *Nn→Neighbor node*
28. *Distance→Dn-Nn (soc)*
29. *Relay_node→Node with minimum distance*
30. *Append Relay_node to Route*
31. *}*
32. *}*
33. *}*
34. *For all the nodes in the network*
35. *Sn broadcast the RTS to the Dn*
36. *End For*
37. *Duplicate_address_list→ Duplicate address list(Dn,NL)*
38. *Add Duplicate_address_list as the destination address in the data packet*
39. *Append route with the data packet*
40. *#Data transmission*
41. *For each 'nr' node in the Route {*
42. *Send data to the node nr*
43. *Foreach entry in Duplicate_address_list {*
44. *If ($nr==$entry)*
45. *Encrypted_dest_addr→last entry in the Duplicate_address_list*
46. *Dest_addr→Decryptted value of Encrypted_dest_addr*
47. *forward data to the destination*
48. *End Foreach*
49. *End Foreach*

In the above algorithm, the function [line 5-9] Duplicate address list has two arguments such as Destination address and Neighbor list of destination node. The Unique ID of each node in the neighbor list is appended into the list dal. The address of the destination is encrypted by using ECC algorithm and stored in the variable E_D_Addr. The secret key is shared with all nodes in the neighborlist by the destination node [line 11-15].Then append with the list dal [line 13]. The source node discovers the route to reach the destination [line 17-33]. The list route has the id of all relay nodes to reach the destination.

Then the source node sends the RTS to the destination to know its availability [line 34-36]. The destination sends back the CTS with the dal. The source adds the dal as the destination address in the data packet and append route with that data packet. The Data transmission process is explained by line [41-49]. The data packet is transmitted via relay node in the route. Each and every relay node checks the presence of its ID in the dal [line 44]. If it is present in the sense, it should be a neighbor of destination. So, it extract the last element of dal, then it decrypt by using secret key to get the destination address [line 46]. Finally forward the received data packet to the destination.

Thus, in our proposed scheme the relay node does not know the destination. The trusted neighbors of destination only have the secret key. So, others cannot know the destination as the destination address is encrypted.

4. SIMULATION RESULTS

The NS2 Simulator is mainly used in the research field of networks and communication. The NS2 is a discrete event time driven simulator which is used to evaluate the performance of the network. Two languages such as C++, OTCL (Object Oriented Tool Command Language) is used in NS2. The C++ is act as back end and OTCL is used as front end. The X-graph is used to plot the graph. The parameters used in the simulation are tabulated as follows:

Table-1. Simulation parameters.

Parameter	Value
Channel type	Wireless Channel
Radio propagation model	TwoRayGround
Network interface type	WirelessPhy
MAC type	IEEE 802.11
Interface queue type	PriQueue
Link layer type	LL
Routing protocol	AODV

The packet delivery ratio, packet loss ratio, end to end delay and throughput are the parameters used in the simulation to evaluate the proposed method.

Packet delivery ratio

The Packet delivery ratio is the ratio of the data packets delivered to the destination successfully. The Packet delivery ratio is one of the important parameter to evaluate the quality of the network. Figure-3 shows the graph for packet delivery ratio analysis.

The formula used to find the Packet delivery ratio is as follows:

$$PDR = \frac{No.of\ packets\ deliverd}{TIme}$$

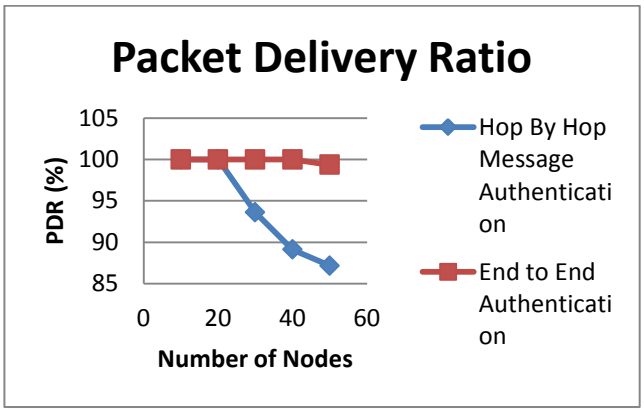

Figure-3. Packet delivery ratio analysis by varying number of nodes.

Packet Loss Ratio

Packet Loss ratio is directly opposite to the Packet Received Rate. The ratio of Number of packets dropped per unit time is called as packet Dropped Rate. The Packet Dropped Rate is calculated by using the formula:

$$PLR = \frac{Number\ of\ packets\ dropped}{Time}$$

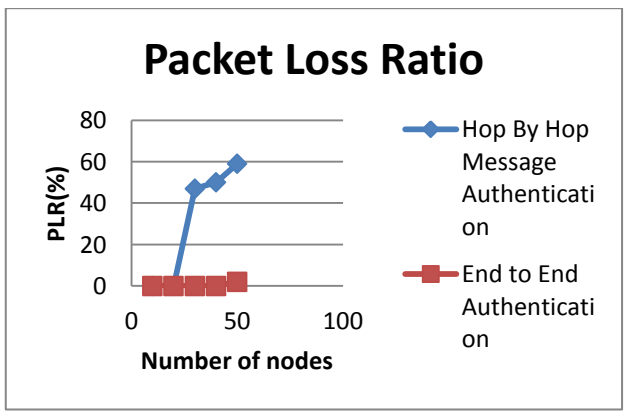

Figure-4. Packet loss ratio analysis by varying number of nodes.

End to end delay

The time taken by the source node to deliver the data successfully to the destination is called as End to End delay. The following formula is used to calculate the End to End delay

$$EndtoEndDelay = {}^{A_T - S_T}/_{n}$$

Where,

A_T A_T →Arrival Time

n→Number of Connections

S_T S_T→Sent Time

Figure-5 shows the graph for end to end delay analysis by varying number nodes.

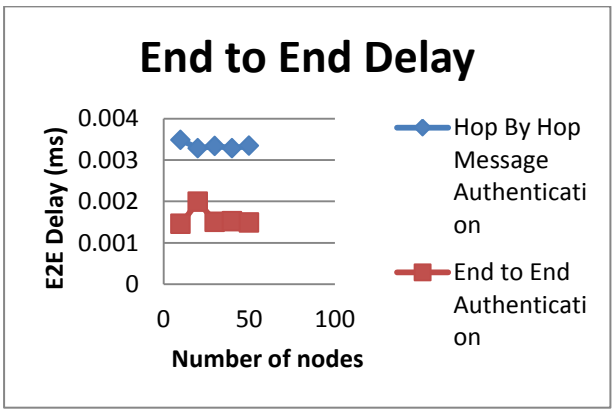

Figure-5. End to end delay analysis by varying number of nodes.

5. CONCLUSIONS

We have proposed a novel anonymous addressing scheme to provide end to end authentication in the Wireless Sensor Network. In the proposed scheme, the hop by hop authentication is provided by using the Elliptic Curve Cryptography (ECC) based Digital signature scheme. The source node sends the message along with signature. Each and every intermediate node should validate the signature to ensure that it receives the message from authenticated node**.** The proposed anonymous authentication scheme ensures the anonymity of destination address from all relay nodes. Simulation results illustrate the effectiveness of our approach.

REFERENCES

[1] F. Ye, H. Lou, S. Lu and L. Zhang. 2004. Statistical En-Route Filtering of Injected False Data in Sensor Networks. Proc. IEEE INFOCOM.

[2] H. Wang, S. Sheng, C. Tan and Q. Li. 2008. Comparing Symmetric-Key and Public-Key Based

Security Schemes in Sensor Networks: A Case Study of User Access Control. Proc. IEEE 28th Int'l Conf. Distributed Computing Systems (ICDCS). pp. 11-18.

[3] W. Zhang, N. Subramanian and G. Wang. 2008. Lightweight and Compromise-Resilient Message Authentication in Sensor Networks. Proc. IEEE INFOCOM.

[4] R. Rivest, A. Shamir, and Y. Tauman. 2001. How to Leak a Secret. Proc. Advances in Cryptology (ASIACRYPT).

[5] S. Zhu, S. Setia, S. Jajodia and P. Ning. 2004. An Interleaved Hop-By-Hop Authentication Scheme for Filtering False Data in Sensor Networks. Proc. IEEE Symp. Security and Privacy.

[6] E. Aivaloglou and S. Gritzalis. 2010. Hybrid trust and reputation management for sensor networks.Wireless Networks. 16(5): 1493-1510.

[7] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung. 1992. Perfectly-Secure Key Distribution for Dynamic Conferences. Proc. Advances in Cryptology (Crypto '92). pp. 471-486.