ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 47 – 50 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp10.pdf

PROVIDING PEER-TO-PEER DATA SECURITY IN WIRELESS SENSOR NETWORKS

P.Poornima[1], M.Pardhasaradhi[2]
[1] M.Tech CSE Student, S.V. Engineering College for Women, Tirupati, India
Poornima.542@gmail.com
[2]Assistant Professor, Dept. of CSE, S.V. Engineering College for Women, Tirupati, India,
pardhasaradhi.m@svcolleges.edu.in

ABSTRACT:
On condition that to provide scalable data security that is having secrecy, accuracy and accessibility in wireless sensor networks is difficult. As a wireless sensor networks consists of a large number of producing constriction sensor nodes that are commonly arrange in unattended or aggressive locations and hence that are exposed to several attacks which are insider attacks. These attacks having node compromise problems. Our Existing system projects that node by node message authentication and privacy of a source in wireless sensor networks, which specifies every forwarder on the routing path must be able to able to check the genuineness and reliability of the message and provide source privacy that means source or sender details are hidden by the network(security server). But it has some constraints that is denial of service such as interrupt attacks with selective forwarding attacks. In this paper we look to avoid these problems for large scale static wireless sensor networks, we come with peer to peer data security framework in which undisclosed keys are bounded to specific geographic location and for each node produce a very few keys those are based on their own location. In our proposed scheme successfully we can restrict compromise nodes and provide node to node authenticity and node to sink authenticity. It is a multifunctional key management framework and also provide en route false data filtering and strongly against denial of service attacks. Our current framework has effective work than existing evaluation in terms of usage of memory, scalability, node compromise resilience.

KEYWORDS- Peer to peer data security, Compromise node attacks, Data security terms

1. INTRODUCTION

Wireless Sensor Networks are huge usage in the present world which is defined as connecting of mobility of users which are having sensing power and it provides information about scientific and an environmental application like temperature etc. In wireless sensor networks, message authentication provides an excellent role to block unauthorized and corrupted message from being forwarded. In cryptography so many authentication frames have been developed.

But on each one having some drawbacks. Those are overcome by our proposed framework. We have two types of cryptosystems symmetric key and public key cryptosystems. Symmetric key cryptosystems requires complex or compound key management, this systems have a lack of scalability that means poor performance and it is only applicable for single compromise node attacks. so that it is useful for single network. These systems are not applicable for multicast a network that means does not work for multicast networks. Here source and destination have to share a key that is secret shared key. The undisclosed key is used by the message sender for data authentication code, that is mutual by a crowd of sensor nodes. An defender can concession the key by a lone sensor node, these troubles are surmount by the public key cryptosystems

Public key cryptosystems having strong key management. Each message is transferred from source to destination with digital signature of that message using the sender private key. Every active routing node that is forwarder or sender at specific location and the final receiver should authenticate the data packet by only using senders public key. In public key schemes having the limitations that is severe computational overheads. Recently one approach was developed for this limitation that is Elliptic Curve Cryptography and it shows that public key schemes can be most helpful in terms of computational complexity and usage of memory and privacy resilience. These schemes have an easy and clean key management. To solve a scalable trouble we will go for polynomial evaluation.

The third scheme is to overcome the problems in public key schemes, polynomial evaluation which was recently developed. This polynomial based scheme is similar to threshold secret sharing. This approach offers information-theoretic security of the shared secret key when the number of messages transmitted is less than the threshold.

The middle nodes checks the accuracy of the data packet through a polynomial evaluation. However, maximum number of messages transmitted than the threshold, the polynomial can be fully recovered and the network is entirely broken.Here we provide an unreservedly effective and efficient source anonymous message authentication

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 47 – 50 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp10.pdf

scheme (SAMA) based on Elliptic curve cryptography. This work based on optimal modified signature scheme on elliptic curves. It contains random oracle model. Randomly pick the nodes on routing path. In our proposed scheme any corrupted message or hacking data packet is detected and dropped by the network and complaint to the source party. In this there is no need to worry about threshold limitation our implemented framework is most effective than polynomial schemes in terms of both theoretical analysis and simulation result analysis.

2. DESIGN GOALS

It seeks to provide peer to peer data safety, as well as en-route fault data filtering in WSNs. In particular, we focus on another task that is event reports created by the sensing nodes that are transferred from the sensing location to the sink node. The below following are the design goals of our system.

2.1 Provide node to node data secrecy and realism:

Both the data secrecy and realism reports must be guaranteed as long as the sending nodes are not compromised. Moreover the impact of compromised nodes (if any) be confined to their surrounding area. In other manner, the intruder cannot utilize the cryptographic things that are like materials accepted from compromised nodes to commence attacks at places other than the area of its compromised nodes.

2.2 Achieve a high-level of assurance on data availability.

High level of assurance means very active belief on data availability that specifies to subsist flexible alongside report interruption attacks and also selective forwarding attacks. It will be able to identify and crash the error records in a deterministic manner that is called as en route capability filtering. The goals are realized in a sole integrated model without relying on other parameters of security infrastructures and it is a simple and efficient while providing peer to peer security and has less and over transmitting the interaction between nodes overheads.

3. RELATED WORK

The previous unidentified interaction protocols are merely compiled from the mix net or DC net. Mix net provides secrecy through data packet reshuffling through a set of mixed servers, in this we have at least one server being trusted. In mix net security server converts from plain text to cipher text of an outgoing message and also ID of the receiver or destination party using the mix net
Public key. Mix net having two operations that is encrypt the data and also decrypt the data. Protocols of Mix net rely on geometric requirements of the background collision but they can't provide executable anonymity results.

DC net is an unknown multi party computation framework. In this very few of the active participants are required to share secret keys. This provides excellent information theoretical source anonymity without requiring the trusted security servers. But one thing at a time one user can send the data so it utilize additional bandwidth to handle contention and collision.

Recently, information source anonymity is based on ring signatures was introduced. This work enables the information sending party to generate a source anonymous message signature with content authenticity assurance. To generate a ring signature, a ring member randomly selects an AS and forges a message signature for all other members. Then he uses his trap-door information to glue the ring together. The novel scheme is very less limited flexibility and very most complexity. However, the novel paper only focused on the relevant cryptographic algorithm.

4. PEER-TO-PEER DATA SECURITY

Scheme Assumptions:

Assume a huge scale identically spreaded wireless sensor network that observes a wide terrain through a big number of static sensor nodes. Here we assume that rough assessment on size and nature of topography is called as priori. Through localization scheme every node can get its geographic location when it is deployed.

We assume that on each event of interest can be detected by numerous sensor nodes. When an event occurs then the sensing nodes are agree on the synthesized report which is forwarded towards the sink node. The sink node traversing a huge number of hops.

Threat Model:

Here sink node is well protected so that it can't be compromised by the attackers or intruders. Suppose an attacker can compromise the multiple nodes at a time then if the node is compromised and also data is stored in that node will be compromised that means information also modified by the attackers and sink node is never be compromised.

5. SELECTION OF ANONYMOUS SET

Selection of anonymous set is very important task here that will shown in below figure.

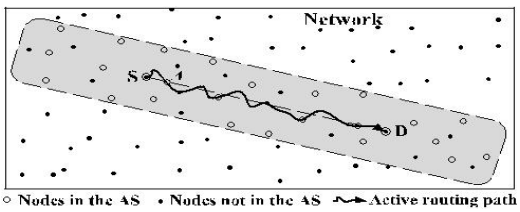

FIGURE 1: Anonymous Set Selection in Active Routing

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 47 – 50 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp10.pdf

6. DETECTION OF COMPROMISED NODES:

We assume that all sensor data will be delivered to a sink node, which can be collocated with the security server. When a data packet is received by the central node that is sink node, source details are hidden by the network. so that we use anonymous set. In anonymous set the message source is hiding. Then the SAMA scheme shows that the reliability of a message is unhampered, if there is any chances to receive bad or meaningless messages from sink node then surely source node is viewed as compromised. If the compromised source node only transmits one message, it will be difficult for node identification without node information. When the compromised node transmits more than one message then the sink node can narrow the compromised nodes down to a very small set.

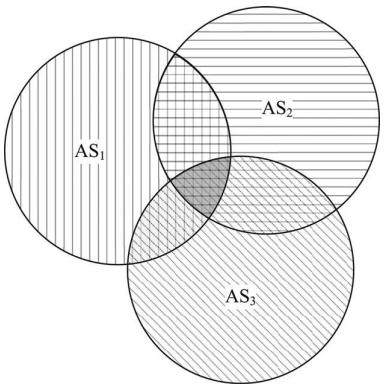

FIGURE 2: Compromised node detection

7. PERFORMANCE ANALYSIS

In performance of our scheme can be achieved by the comparison of both theoretical and simulation results.

7.1 Theoretical Analysis

Manage**ment** of key is one of the major issues of

Secret key based authentication schemes. it is essential for wireless sensor networks. While many of these schemes can be designed to provide node by node authentication by using secret shared key between source and destination.

The receiver should verify the authenticity of the message that means there is no intermediate checking of a message. so that hop by hop authentication was proposed. if there is any mistake or meaningless message forwarded by any node, that message will be dropped to conserve the sensor energy. this task consumes more sensor power as well as increase the network collision ratio and decreases the message delivery ratio.

In addition to perform to overcome denial of service attacks and wavelength allocation of a wireless sensor networks calculated by using below formula.

$$f(x,y) = \sum_{i=0}^{d_x} \sum_{j=0}^{d_y} A_{i,j} x^i y^j,$$

7.2 Experimental Results

In this section, we implement the polynomial based scheme and our proposed scheme in a real world comparison. The comparison is based on comparable security levels.

The implementation was carried out on Mica2 plat-form, which is 8 MHz, while our implementation is carried out on Telosb platform, which is 4 MHz We first provide simulation in Table 1 to compare and justify our parameter selections. From the table, we can see that our results is comparable with the original paper. This justifies that the performance comparisons between our scheme and the algorithm proposed in using different parameters are consistent and reasonable.

(a). Original implementation [4]							
$d_x, d_y = 3$				$d_x, d_y = 4$			
ROM (KB)	RAM (B)	Sign (ms)	Verf (ms)	ROM (KB)	RAM (B)	Sign (ms)	Verf (ms)
14.78	1938	5.8	57.89	15.04	2211	7.59	70.8
(b). Our implementation							
$d_x, d_y = 3$				$d_x, d_y = 4$			
ROM (KB)	RAM (B)	Sign (ms)	Verf (ms)	ROM (KB)	RAM (B)	Sign (ms)	Verf (ms)
13.61	1938	9	108	13.65	2302	11.73	126.93

8. RESULT

The final result of our proposed scheme is to provide secure energy and to provide scalable large delivery ratio. Peer To Peer networks mainly useful for linear transmissions. But it has neighboring compromised nodes problem. The following graphs shows that, these drawbacks are in our existing system that should be solved by using SAMA scheme based on Elliptic curve cryptography (Modified Elgamal Signature scheme) On every basis of our final result, proposed scheme is more efficient than existing system in terms of consumption of energy, delay of message and delivery ratio.

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 47 – 50 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp10.pdf

9. CONCLUSION

In our paper we proposed an effective and novel SAMA based on ECC. This helps us to authenticate the message. It is very helpful in future also. no need to worry about threshold problem. In this we can forward any number of messages and it is a fast transaction method. Already we discuss about compromise node attacks. We have a few extensions also, by exploiting the stable location of a wireless sensor networks that provide peer to peer data security. The network is to provide several types of keys which are having secrecy. That provide end to end data security frame work to address vulnerabilities in our existing system. In this each node stores small number of keys that is based on their own location. Our proposed scheme is multifunctional key management. This ensures both node to sink and node to node authentication along with routes forwarding. This scheme filters the bogus data and also against of denial of service attacks. Finally we evaluate our proposed scheme with extensive methodology. It has a peek resilience against an increasing maximum number of compromised nodes and efficiency of protocol overheads.

REFERENCES

[1] D. Carman, P. Kraus, B. Matt, .Constraints and approaches for distributed sensor network security,. NAI Labs Tech. Report #00-010, 2000

[2] A. Wood and J.Stankovic, .Denial of Service in Sensor Networks, IEEE Computer, Oct. 2002.

[3] C. Karl of and D. Wagner, .Secure routing in Wireless Sensor Networks: Attacks and Countermeasures. , Ad Hoc Networks, 1(2), 2003.

[4] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, .SPINS:Security Protocols for Sensor Networks,. In Proc. of Mobicom 2001.

[5] Elaine Shi and A. perrig, .Designing Secure Sensor Networks,. Wireless Communication Magazine, 11(6), December 2004.

[6] L. Eschenauer and V. Gligor, .A key-management scheme for distributed sensor networks,. In Proc. of the 9th ACM CCS, Washington, 2002

[7] H. Chan, A. Perrig, .Security and privacy in sensor networks,. IEEE Computer, pp. 103-105, Oct 2003

[8] R. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[9] P.Poornima and M.Pardhasaradhi “hop by hop message authentication and source privacy in wsns” vol 25 no.5 may 2014.