Trusted Lightweight Authentication Protocol used in Wireless Sensor Network

Pranjali P. Koli
PG Student [Communication Network]
D. Y. Patil College of Engineering
Akurdi

D.G. Khairnar, Ph.D
HOD, Dept. of Electronics and Telecommunication
D. Y. Patil College of Engineering
Akurdi

Trupti Wagh
Dept. of Electronics and Telecommunication
D. Y. Patil College of Engineering
Akurdi

ABSTRACT

Secure data transmission is essential in Wireless Sensor Network (WSN) to protect sensitive communications in the network. To improve the security of such network, this project proposes a successful routing among authentic nodes with adversary nodes inside the network, and forms the secure wireless sensor network. The authentication protocol will enable the receiving end to affirm that the packet has originated from a genuine node. It will preserve the integrity as well as authentication and confidentiality. Impersonation attack can be prevented in which a node will pretend like other node and sends the request to base station. Trust values to nodes make it more secure system. Performance of the proposed system evaluated based on the parameters such as delay and transmission overhead. General Terms

Keywords

WSN, authentication, trust, impersonation attack, Chinese Remainder Theorem, encryption

1. INTRODUCTION

A Wireless sensor network (WSN) is composed of a large number of sensor nodes, which can be densely deployed either inside the phenomenon or close to it. Some of the applications of the WSN are health, military, and security. The sensors can communicate to each other through wireless links, and most of the times they use radio frequency channels for the purpose of communication. Sensors are very simple identical electronic devices equipped with a processor and small storage memory and a communication channel. WSN networks are made of several hundred to several thousand of sensors propagated in a geographical area. Most of the times it is desired to collect the data of all sensors in a specific station for processing and other purposes. The station is a data sink, and it has large processing power, storage space, and it has capability of communicating to the sensors.

There are many sensor network applications like such environmental data collection, security monitoring, military, medical, tracking etc. when sensor networks are randomly deployed in a hostile environment, security becomes extremely important factor. Because sensed data of sensor nodes is prone to different types of malicious before reaching base station. Security mechanisms are needed in communication part of the networks to provide safe data. The security is very important concern to get full advantageous of in-network data processing sensor networks. Protecting sensed data is complicated task. Even through wireless sensor network is an advanced technology of network, it is very different from traditional wireless networks. This is, due to the unique characteristics of sensor nodes in WSN. So existing security mechanisms of traditional wireless networks are not directly applied in WSN. Sensor networks are closely interacting physical environment. So sensor nodes are also deployed in all areas even physical accessible attacks and broadcasting sensed data in network. So these reasons give a scope to new security mechanism rather than applying existing traditional security mechanisms in WSN.

2. PRIOR WORK

Several authentication protocols have been proposed to prevent breach of system in a wireless sensor network. These authentication protocols generally involve complex computations and require a larger memory space. In [1] author proposed a short signature scheme based on the Computational Diffie-Hellman assumption on certain elliptic and hyper-elliptic curves. The signature length size is half the size of a DSA signature for a similar level of security. Their system proposed a signature scheme whose length is approximately 160 bits and provides a level of security similar to 320-bit DSA signatures. This signature scheme is secure against existential forgery under a chosen message attack (in the random oracle model) assuming the Computational Diffie-Hellman problem (CDH) is hard on certain elliptic curves over a finite field of characteristic three. Advantage of this schemes is short signature scheme generates the signatures are sent over a low-bandwidth channel but disadvantage is that short signature does not support confidentiality and non reputation.

In [2] explained security mechanisms that are widely used and proven to be effective in wired networks are not always applicable to MANETs. Attacks that can be effectively detected and prevented in wired networks have been big security challenges in MANETs. It has many advantages like it is easier to deploy without any infrastructure requirement. The public key of IBC is self-proving and can carry much useful information and its resource requirements, regarding process power, storage space, communication bandwidth, are much lower. Along with these advantages it has many disadvantages too. The proposed technique IBC does not ensure the authentication between the sender and receiver.

In [3] developed a multilevel key chain scheme to efficiently distribute the key chain commitments for the broadcast authentication scheme named μTESLA. By using pre-determination and broadcast, this approach has removed µTESLA's requirement of a unicast based distribution of initial key chain commitments, which introduces high communication overhead in large distributed sensor networks. They also proposed several techniques, including periodic broadcast of commitment distribution messages and random selection strategies to make improvement in the survivability of this scheme and defeat some DOS (Denial Of Service) attacks. The resulting protocol, named multilevel µTESLA, satisfied several nice properties which includes low overhead, tolerance of message loss, scalability to large networks, and resistance to replay attacks as well as DOS attacks. In µTESLA the key is effectively distributed. It has high scalability and low overhead. But it does not provide the authentication and message integrity.

In [4] proposed an authenticated pair wise and broadcast communication scheme which uses pairing-based cryptography. The pair wise scheme used requires only private keys to be generated by the Trusted Authority (TA). Users can generate their pair wise symmetric keys non-interactively, provided the identities of users are either published by the TA or sent with the message by the sender. In order to reduce bandwidth overhead caused by pair wise communication in case of broadcast messages, this system proposed pairing-based signcryption scheme for an authenticated broadcasting. It has identity-based pair wise symmetric keys used to authenticated pair wise communication in ad hoc network and pairing-based signcryption scheme for authenticated broadcasting. It does not suitable for adaptable MANETs.

In [5] proposed a novel anonymous on demand routing protocol is called as MASK, to enable both anonymous MAC layer and network-layer communications so as to thwart adversarial, passive eavesdropping and the resulting attacks. MASK provides anonymity in neighbourhood authentication, route discovery, and packet forwarding. The proposed technique MASK has not proved that defend against the DOS attacks and mobile attacks. But it does not provided to ensure both routing anonymity and strong routing security. Digital signature scheme is based on the computational difficulty of integer factorization.

In [6] scheme possesses the novel property of being robust against an adaptive chosen-message attack: an adversary who receives signatures for messages of his choice (where each message may be chosen in a way that depends on the signatures of previously chosen messages) cannot later forge the signature of even a single additional message. Digital signature scheme is robust against an adaptive chosen-message attack. The proposed technique does not ensure the authentication between the sender and receiver.

In [7] the proposed system describes an ID based authenticated two pass key agreement protocol which makes use of the Weil pairing. Key agreement is one of the fundamental cryptographic primitives after encryption and digital signatures. The main aim of the protocol is describes that the ability to add key conformation in the secure key sharing mechanism. Key agreement protocol is only concerning the sharing of secure key, but it is not implementing the security features for confidentiality and non reputation.

3. PROPOSED SYSTEM

The main proposal of the lightweight authentication protocol is to ensure better performance in the core of the sensor network. In WSN, authentication of Nodes is extremely important.

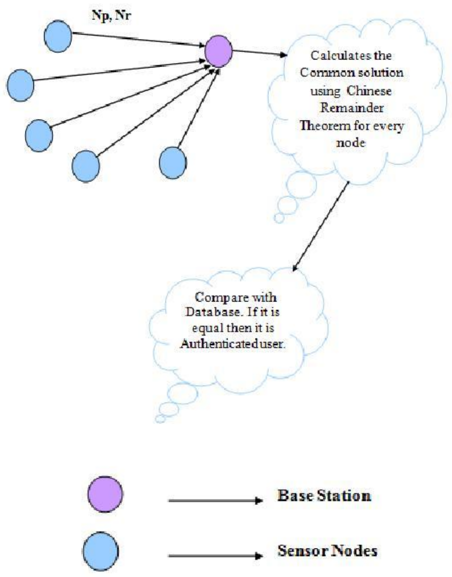

Np, Nr
Calculates the Common solution using Chinese Remainder Theorem for every node
Compare with Database. If it is equal then it is Authenticated user.
Base Station
Sensor Nodes

Fig 1: System architecture

In this proposed system, there are two types of communication that take place within the sensor network, one which involves a Sensor node sending data to Base station and another involves the base station sending all the data to database server which is linked through some external network. During data communication between the sensor nodes to base station or base station to database server the authentication is most important. To achieve secure communication in WSN, routing protocol must encapsulate an essential set of security mechanisms. These are mechanisms that help prevent, detect, and respond to security attacks. Authentication enables communication parties could identify with each other. Therefore, an adversary cannot masquerade a node to gain sensitive resources. Initially, trust value of all nodes is maintained as high value that means if the misbehaving node is detected its trust value can be reduced. The authorized user keeps the information sent unreadable to unauthorized users or nodes. To keep the information is authentication, the sensor node, base station and data server uses the private and public key pair for encryption and decryption. The public key is used to provide encrypt the data and corresponding private key is provided for decryption. The impersonation attack can be prevented in which a node will pretend like other node and sends the request to base station. At the base station this attacker can be easily detected because attacker node does not the secret Np, Nr information. If the node is detected as authenticated user its trust value is high.

Impersonation attacks in wireless and sensor networks by professional criminal groups are becoming more sophisticated. An attack in which a hostile sensor node system masquerades as a trusted sensor node is impersonation attack. Through impersonation attack a node can launch flooding attack.

Sensor node sends the request to the base station along with Np, Nr. The base station Base Station computes the common solution using Chinese Remainder Theorem (CRT) for every node using parameters Np, Nr, Bp, Br. Np, Nr are delivered to the node by the BS during registration process. All the information is stored in database of BS.

Np - prime number of a node

Nr - Residue of a node

Bp - prime number in BS corresponding to node

Br - Residue in BS corresponding to node

At the base station, the request is instantly received and authentication verification is done using Chinese Remainder Theorem (CRT). Using received Np, Nr and Bp, Br, BS computes the common solution and compare with that stored in database. If it matches it is authenticated node. Otherwise it is not authenticated user node.

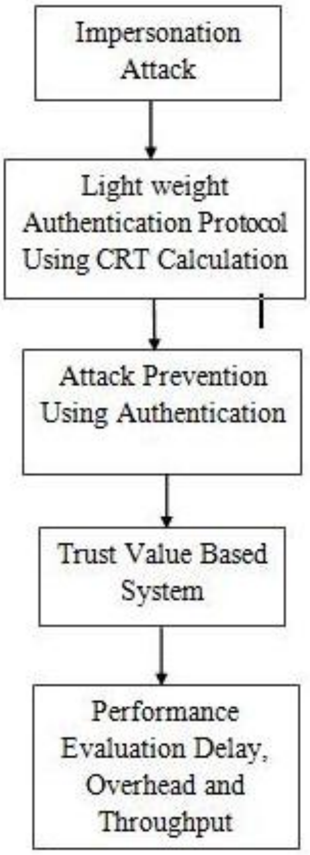

Impersonation Attack
Light weight Authentication Protocol Using CRT Calculation
Attack Prevention Using Authentication
Trust Value Based System
Performance Evaluation Delay, Overhead and Throughput

Fig 2: Block Diagram

The data that has been sent from the sensor is encrypted and decrypted at the receiving end. The authentication mechanism the attacker is performed by the source node only can be detected not intermediate route. Such kind of attack is impersonation attack. Hence using authentication, impersonation attack can be prevented in which a node will pretend like other node and sends the request to base station. At the base station this attacker can be easily detected because attacker node does not know the secret Np, Nr information. Simulation environment is as shown in Table 1.

4. RESULTS

Delay is the time taken for a packet to reach the destination from the source node.

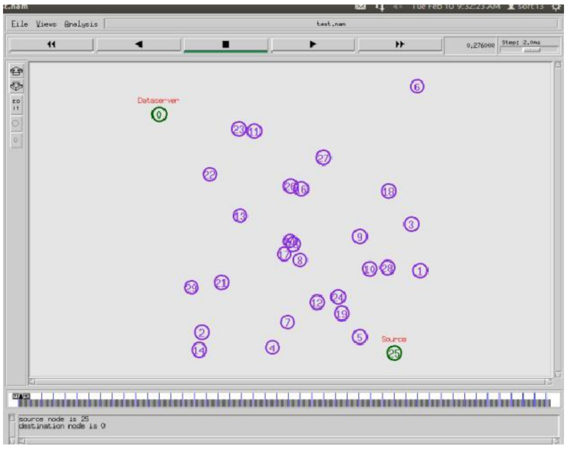
$$Delay\ (ms)\ = \frac{\sum (Delay\ of\ each\ entities\ data\ packet)}{Total\ number\ of\ delivered\ data\ packets}$$

Throughput: It is the amount of time taken by the packet to reach the destination.

Table 1. Simulation Environment table

Simulator	Network Simulator 2
Number of Nodes	Fixed
Topology	Random
Interface type	Phy/WirelessPhy
Mac type	802.11
Queue type	Drop tail/Priority Queue
Queue Length	200 Packets
Antenna type	Omni Antenna
Propagation type	Two ray Ground
Routing Protocol	AODV
Transport Agent	UDP
Application Agent	CBR
Transmission Power	2.0
Reception Power	1.0
Idle Power	0.0watts
Initial Energy	Random
Simulation Time	50seconds

Throughput (bits/s) = Total Data / Data Transmission duration.



```
source node is 25
destination node is 0
```

Fig 4: Creation of source and data server

From figure 5, figure 6 and figure 7 it can be seen that this proposed protocol is having lesser end to end delay, lesser packet delay and because of that overall throughput gets increased.

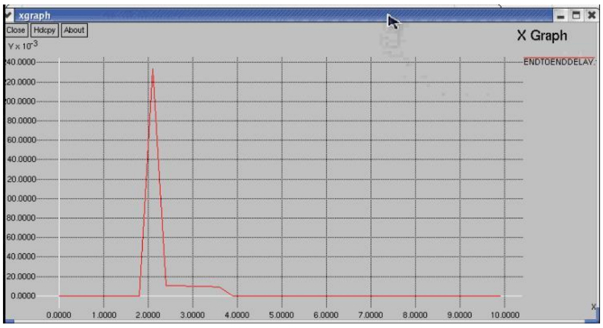


Fig. 5. End to end delay

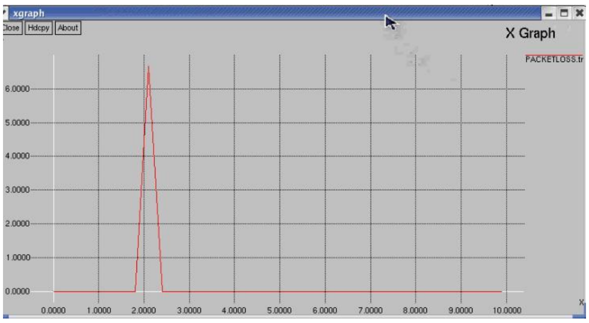


Fig. 6: Packet Delay

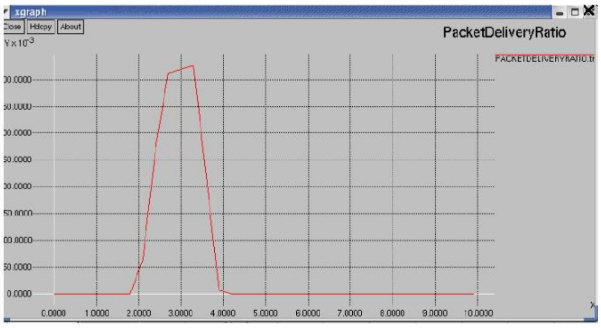


Fig 7: Packet Deliver ratio

5. CONCLUSION

Proposed authentication mechanism and secure routing scheme is robust against the vulnerable to various attacks. The proposed protocol is efficient and better against impersonation attack. This project contributes trust value based system in authentication. The performance of the network is evaluated from the simulation in terms of delay, throughput, transmission overhead, no of packets generated and received and they are found to be better than previous ones.

6. REFERENCES

[1] D. Boneh, B. Lynn, H. Shacham, Short signatures from the weil pairing, in: Proc. ASIACRYPT, LNCS, Springer, 2001, pp. 514–532.

[2] S. Zhao, A. Akshai, R. Frost, X. Bai, A survey of applications of identity-based cryptography in mobile ad-hoc networks, IEEE Communication. Tutorials Early Access (2011) 1–21.

[3] D.Liu and P.Ning, "Multi-level µTESLA: Broadcast authentication for distributed sensor networks," ACM Transactions in Embedded Computing Systems (TECS), vol.3, no.4, 2004

[4] M.J. Bohio, A. Miri, An authenticated broadcasting scheme for wireless ad hoc network, in: Proc. CNSR 2004, IEEE Computer Society, 2004, pp. 69–74.

[5] Y. Zhang, W. Liu, W. Lou, Y. Fang, MASK: anonymous on-demand routing in mobile ad hoc networks, in: Wireless Commun., IEEE, 2006, pp. 2376–2385.

[6] S. Goldwasser, S. Micali, R.L. Rivest, A digital signature scheme secure against adaptive chosen-message attacks, J. SIAM Comput. 17 (April) (1988) 281–308.

[7] N.P, An Identity-based Authenticated key agreement protocol Based on the Weil Pairing, in: Dept of Computer Science University of Bristol Merchant Venturers Building Woodland Road_Bristol BS_UB, pp.1–6.

[8] Mark Hempstead, Michael J. Lyons, David Hardware Systems for Wireless Sensor Networks, "Journal of Low Power Electronics Vol.4, 1–10, 2008

[9] Jianmin Zhang , Wenqi Yu and Xiande Liu, "CRTBA: Chinese Remainder Theorem- Based Broadcast Authentication in Wireless Sensor Networks," in Computer Network and Multimedia Technology, 2009, Wuhan, International Symposium on 18-20 Jan. 2009.

[10] Mark Hempstead, Michael J. Lyons, David Hardware Systems for Wireless Sensor Networks, "Journal of Low Power Electronics Vol.4, 1–10, 2008.