Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 8; April-June, 2015 pp. 66-70
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/acsit.html

Trusted Lightweight Authentication Protocol used in Wireless Sensor Network

Pranjali Koli[1], D.G. Khairnar[2] and Manish Sharma[3]

[1,2,3]Dept. of E&TC, D Y Patil College of Engineering, Akurdi, Pune.
E-mail: [1]pranjalikoli55.pk@gmail.com, [2]dgkhairnar1975@gmail.com,
[3]manishsharma.mitm@gmail.com

Abstract—*Security of wireless Sensor Network (WSN) is very essential to protect sensitive communication in network. For this a new lightweight protocol to authenticate a node in WSN is proposed. It uses Chinese Remainder Theorem (CRT) to authenticate a node in WSN. During registration phase secret values distributed to nodes by Base Station (BS) and by using CRT, common solution is stored at BS which is used to compare with solution from requested node to identify genuine node and attacker node. It overcomes impersonation attack in which a hostile sensor node masquerades as a genuine sensor node. Proposed system overcomes flooding in the network which is caused by impersonation attack. Encryption decryption of data makes system confidential. One more feature of trust value also added which makes system more secure.*

Keywords*: WSN, authentication, trust, impersonation attack, Chinese Remainder Theorem, encryption.*

1. INTRODUCTION

WSN consist of distributed wirelessly enabled embedded devices with different electronic sensors. Each node in WSN is equipped with one or more sensors with a microcontroller, transceiver and energy source. Now a day's WSN being used throughout the world as they gives a wide range of applications like intelligent buildings, home security, medical health care, etc. WSN have one more Base Station (BS) which decides routes in the network. All the nodes are connected to the base station. Two types of communication present in WSN. One is between nodes and BS. Second is between BS to database server. Sensor networks actively monitor the surroundings and it is essential to provide security in order to prevent leakage of information.WSN facilities eavesdropping, packet injection by third party. So it is very necessary to maintain confidentiality of information so that third party cannot be able to decrypt the information.

There are three major security aspects that need to be addressed to maintain security in WSN. These three attributes are:

1) Authentication

It enables communication parties to identify each other so that adversary cannot masquerades a node.

2) Confidentiality

It ensures that information is never disclosed to unauthenticated entities.

3) Integrity

It guarantees that information being transferred is never altered. Only authenticated nodes are able to modify the information.

Sensor node is usually equipped with limited energy resources according to application area. Asymmetric cryptographic method (e.g. the RSA algorithm, digital signature) is often too expensive and gives out high overhead which is to be avoided in WSN. Another method is symmetric cryptographic method (e.g. AES block cipher or the HMAC-SHA-1 message authentication code) is faster to compute but complicates the design of secure application and if third party knows the shared key it can access the data from sensor node.

Two types of attacks are there in WSN these are passive attack and active attack.

Passive attack: This attack targets to confidentiality of the system. These attacks are generally used to gather the information about network or to know communication pattern between communicating parties.

Active attack: This attack attempts to alter or modify data being exchanged in the network. In this attack intruder can modify the packets, inject the packets, drops the packets or it can use various features of network to launch the attack. Active attacks are very dangerous.

Impersonation attack is one of the active attack in which a node pretend like other node and sends the request to the base station. Impersonation attack leads to flooding attack in network which makes down performance of network.

Our proposed system is trust value based system. Trust value of all nodes is maintained at high value means at 1. If misbehaving node is detected its trust value can be reduced to zero. Trusted nodes will be taken into account while routing which makes our system more secure.

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. Short signature does not support confidentiality and non reputation.

In [2] developed a multilevel key chain scheme to efficiently distribute the key chain commitments for the broadcast authentication scheme named µTESLA. 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. 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 [3] 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). 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 (Mobile Ad-hoc Networks) MANETs.

In [4] authors discussed different issues and mechanisms to achieve secure communication. They discussed the threat and base-station-based trust model. They discussed different security requirements and countermeasures to the attacks. In [5] the security issues, threats and attacks and requirements of wireless sensor networks had analyzed. They proposed security framework and security architecture to integrate existing technologies with WSN technology, to provide secure and private communications to its users. In [6] authors presented a two-factor user authentication protocol for WSN, which provides strong authentication, session key establishment. Two phases had mentioned, first is registration phase and second is authentication phase. Authentication phase is further divided into login and verification phase by using Hash function.

In [7], a hybrid Key predistribution scheme that supports spatial retreat strategies to cope with jamming attacks is proposed. This scheme combines the properties of random and deployment knowledge based key predistribution schemes. They proposed a solution for robust key distribution to cope with node movement to counter jamming attacks. In [8] presented two new broadcast authentication schemes, called the key pool scheme and the key chain scheme, to solve this dilemma without any synchronization or periodic key redistribution. Both schemes utilized a bloom filter.

In [9] proposed a Lightweight and Dependable Trust System (LDTS) for WSNs, which employ clustering algorithms. A lightweight trust decision-making scheme is proposed based on the node's identities (roles) in the clustered WSNs, which is suitable for such WSNs because it facilitates energy-saving. In [10] authors identified an inherent design weakness in the user preprocessing phase of Secure and Distributed Reprogramming Protocol (SDRP) and demonstrated that it is vulnerable to an impersonation attack.

3. PROPOSED SYSTEM

In this paper a new protocol which can be used in WSN for authentication of sensor nodes is proposed and which will give lower overhead in terms of energy consumption and packets drops. Block diagram of our proposed system is shown in fig.1 in which impersonation attack will get overcome by authentication in which CRT is used to store common solution. Our proposed authentication protocol works in two phases: Registration and Authentication.

Registration phase: During the registration BS gives the Np, Nr value to each sensor node which can be again saved in database of BS as Bp, Br.

Np: Prime number of a node.

Nr: Residue number of a node.

Bp: prime number in BS corresponding to node.

Br: Residue number in BS corresponding to node.

e.g. For node 1, set Np (1) 29

set Nr (1) 2

set CRT (1) 524

Fig. 2 shows the basic architecture of our proposed system in which sensor node sends the request to BS along with its Np, Nr value. Authentication enables communication parties could identify with each other. Therefore, an adversary cannot masquerade a node to gain sensitive resources.

Authentication Phase: Sensor node sends request along with Np, Nr to the base station. Then base station computes the common solution using CRT and make compares with that solution stored in database. If it matches then it is an authenticated node otherwise it is unauthenticated node.

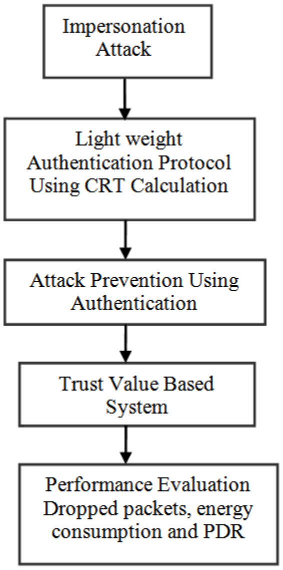

Impersonation Attack
Light weight Authentication Protocol Using CRT Calculation
Attack Prevention Using Authentication
Trust Value Based System
Performance Evaluation Dropped packets, energy consumption and PDR

Fig. 1: Block Diagram

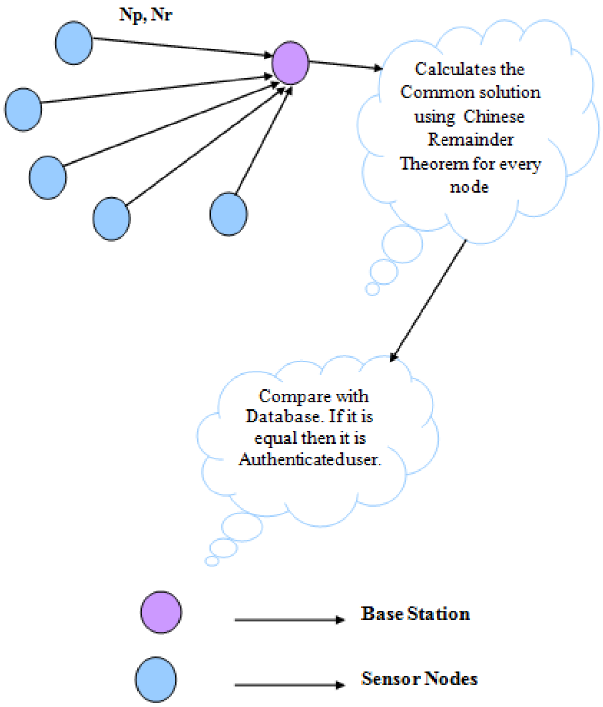

Np, Nr
Calculates the Common solution using Chinese Remainder Theorem for every node
Compare with Database. If it is equal then it is Authenticated user.
Base Station
Sensor Nodes

Fig. 2: System architecture

Impact of proposed protocol on impersonation attack

In impersonation attack a hostile sensor node system masquerades as a trusted sensor node. Through impersonation attack a node can launch flooding attack. In this attack attacker sends the request to the base station with Np, Nr value and ID value (identity value) of victim node. When request received at BS calculation common solution from CRT is done. As the attacker does not know secret Np, Nr value of victim node common solution does not matches at BS. It will be then marked as unauthenticated node and its trust value will be 0. Once the node marked as unauthenticated node all the further communication with that node stops hence leakage of information and flooding due to continuous sending of packets from unauthenticated node gets stopped.

Trust value based system

Initially, trust value of all nodes is maintained as high value (e.g. 1), if the misbehaving node is detected its trust value can be reduced (e.g. 0). Trust value of nodes taken into account while routing. Nodes with trust value 0 are avoided in routing so as to avoid leakage of sensitive information which makes our system more secure.

Encryption and decryption

The authorized user keeps the information sent unreadable to unauthorized users or nodes. The data that has been sent from the sensor is encrypted and decrypted at the receiving end.

At source node,

Data to be sent + secret CRT value = Encrypted data.

At receiving node:

Encrypted data – Secret CRT value= decrypted data.

4. RESULTS& DISCUSSION

NS-2 (Network Simulator version 2) is used to simulate proposed protocol.

Table 1: Simulation environment

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

Different simulator parameters are shown in following TABLE I.

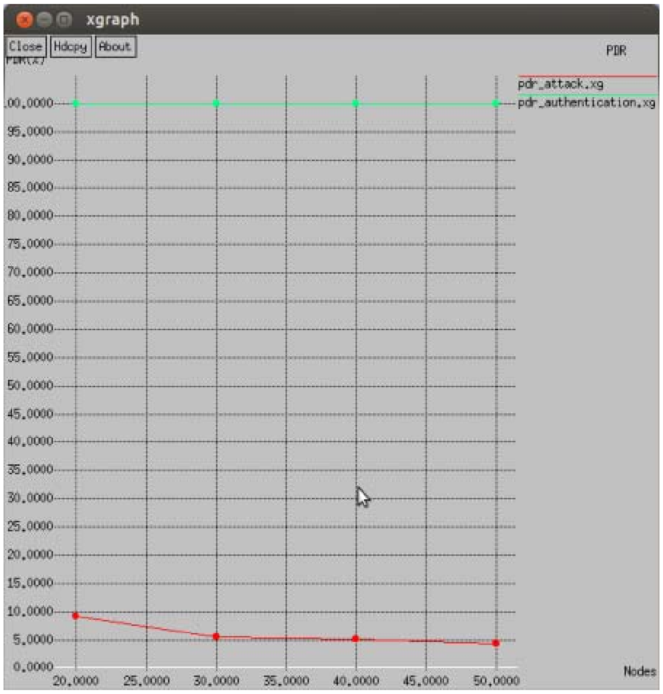


Fig. 3: Packet Delivered Rate

As shown in graph of fig.3, on X-axis number of sensor nodes. Nnumber of sensor nodes aew 20, 30, 40, 50 and a random topology selected . PDR under attack in the network is much lesser than PDR after authentication process. Due to the authentication process attackers are filtered in the network.

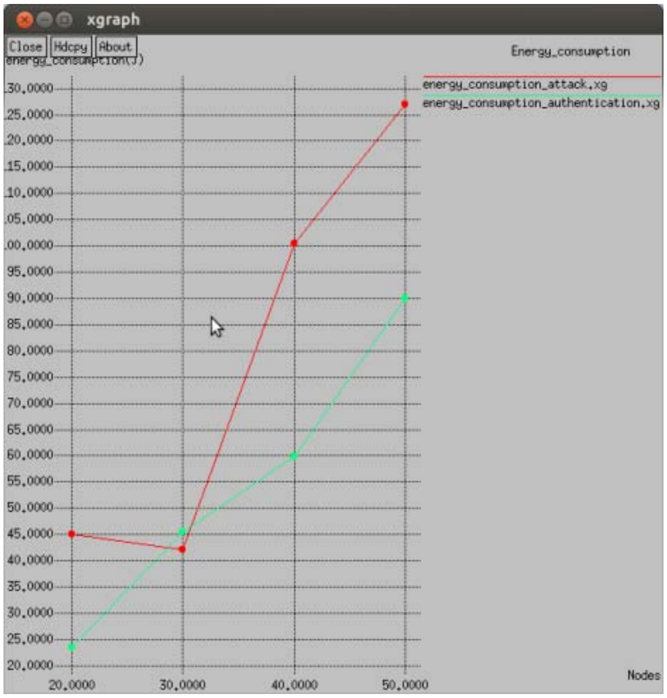


Fig. 4: Energy consumption

As shown in fig.4, energy consumption under attack is increased due to the flooding attack. It is lesser after authentication due to the attack prevention.

As shown in fig. 5 , dropped packets under attack in the network is much higher than Dropped packets after authentication process. Due to the authentication process attackers are filtered in the network.

As shown in fig.6, source 24 impersonates 20 and launches flooding attack which creates packet loss and high energy consumption in the network

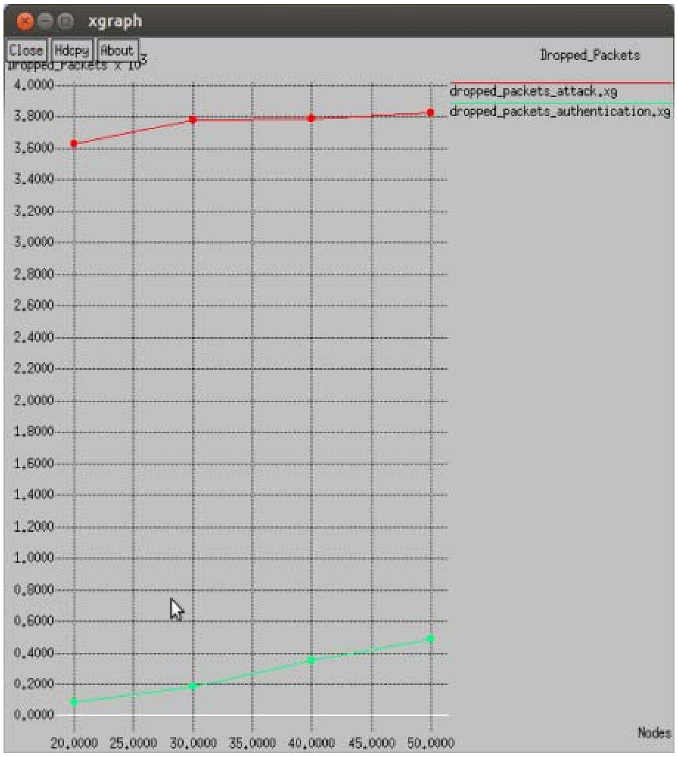
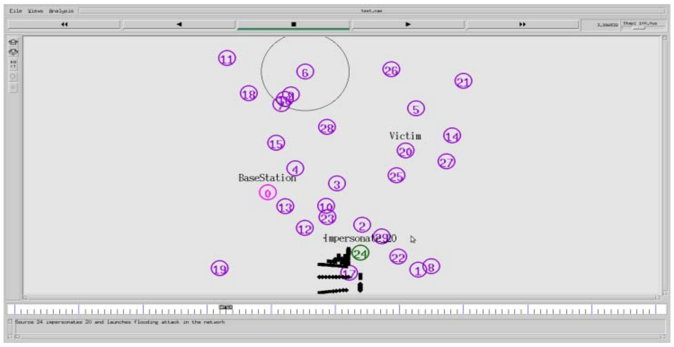


Fig. 5: Dropped Packets



Source 24 impersonates 20 and launches flooding attack in the network

Fig. 6: Dropped Packets

5. CONCLUSION

Proposed authentication mechanism and secure routing scheme is robust against various vulnerable attacks. The proposed protocol is efficient and better against impersonation attack. This project contributes trust value based system in authentication which makes the system more secure. The performance of the network is evaluated from the simulation in terms of PDR, energy consumption and dropped packets.

REFERENCES

[1] D. Boneh, B. Lynn, H. Shacham, “Short signatures from the weil pairing”, in preceding to ASIACRYPT, LNCS, Springer, vol.5, no.7, pp. 514–532,2001.

[2] D.Liu, P.Ning, “Multi-level µTESLA: Broadcast authentication for distributed sensor networks”, ACM Transactions in Embedded Computing Systems (TECS), vol.3,no.4, pp. 21-36, 2004.

[3] M.J. Bohio, A. Miri, “An authenticated broadcasting scheme for wireless ad hoc network”, in preceding to CNSR, IEEE Computer Society, vol.9, no.4, pp. 69–74, 2004.

[4] Elaine Shi, Adrian Perrig, Carnegie Mellon University, “Designing Secure Sensor Networks”, IEEE Wireless communications , vol.3, no.7, pp.26-34, 2004.

[5] Neeli R. Prasad, Mahbubul Alam “Security Framework for Wireless Sensor Networks”, Springer Wireless Personal Communications, vol.2, no.4, pp. 455–46, 2006.

[6] Manik Lal Das, Member, IEEE, “two-factor User Authentication In Wireless Sensor Networks”, IEEE Transactions On Wireless Communications, vol.8, no.3, pp.57-65, 2009.

[7] Korporn Panyim, Prashant Krishnamurthy, “A Hybrid Key Predistribution Scheme for Sensor Networks Employing Spatial Retreats to Cope With Jamming Attacks”, SpringerMobile Netw Appl vol.5, no.9, pp.327–341, LLC, 2012.

[8] Panoat Chuchaisri, Richard Newman. “Fast Response PKC-based Broadcast Authentication In Wireless Sensor Networks”, published online springer, vol.2, no.9, pp.45-57, LLC, 2012.

[9] Xiaoyong Li, Feng Zhou and Junping Du. “LDTS: A Lightweight and Dependable Trust System for Clustered WirelessSensorNetworks”, IEEE Transactions On Information forensics and Security, vol. 8, no. 6, pp.34-45, 2013.

[10] Huei-wen Ferng , Jeffrey Nurhakim and Shi-jinn Horng, “Key Management Protocol With End-to-end Data Security and Key Revocation for A Multi-BS Wireless Sensor Network”, Springer Wireless Netw, vol.6, no.20, pp .625–637, 2014.

[11] Balamurugan,dr.R.Poongodi, “Effective Lightweight Trust Decision Making Scheme for Wireless Sensor Networks”, Journal of Theoretical and Applied Information Technology, Vol. 67 No.3, pp.123-132, 2014.

[12] U. Senthil Kumaran, P. Ilango, “Secure Authentication and Integrity Techniques for Randomized Secured Routing In WSN”, Springer Wireless Netw , vol.5, no-4, pp.443–451, 2015.