ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 5, May 2015

A Security Enhanced Group Signature Based Authentication in ZIGBEE Networks

Binoy Babu M [1], P.M. VijayKumar [2], Divya Nair D [3]

PG Scholar, Dept. of ECE , Maharaja Prithvi Engineering College, Avinashi,Chennai, Tamilnadu,,India [1]

Assistant professor, Dept. of ECE, Maharaja Prithvi Engineering College, Avinashi, Chennai, Tamilnadu, India[2]

PG Scholar, Dept. of ECE , Maharaja Prithvi Engineering College, Avinashi,Chennai, Tamilnadu, India[3]

Abstract: The IEEE 802.15.4 is a new standard defined for LR-WPAN which provides a low cost and very less complicated solution. The targeted applications are wireless sensors networks (WSN), interactive toys, home automation and remote controls. ZigBee is one of the newest technologies developed by ZigBee Alliance, enabling Wireless Personal Area works (WPAN). ZigBee is the name of a specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4 standard. New techniques of security measures are essential for high-survivability network. The group signature scheme implemented by combining the parameter exchange of Diffie-Hellman algorithm into the handshake protocol for node's joining a ZigBee network. The major improvement of Diffie-Hellman algorithm is to mix the parameters of key exchange operation so as to defend against typical man-in-the-middle attacks. Through the security analysis, the group signature scheme demonstrates stronger security. We can verify that the ZigBee routing protocol with security enhancement has larger flexible application in wireless networks.

Keywords: ZigBee, Diffie-Hellman, Group Signature, Key management

I. INTRODUCTION

ZIGBEE is the emerging industrial standard for ad hoc networks based on IEEE 802.15.4. Due to characteristics such as low data rate, low price, and low power consumption, ZIGBEE is expected to be used in wireless sensor networks for remote monitoring, home control, and industrial automation. Since one of the most important goals is to reduce the installation and running cost, ZIGBEE stack is embedded in small and cheap micro-controller units. Since tree routing does not require any routing tables to send the packet to the destination, it can be used in ZIGBEE end devices that have limited resources.

For an unsecured network, an attacker could modify and inject messages to cause a network error or industrial harm. Meanwhile, many applications also require confidentiality and most have a need for integrity protection. Secure communication is a key for any wireless network. Like all other networks, ZigBee are susceptible to various kinds of attacks like DOS attack, PUE attack, tunnel attack and jamming attack. Anonymous communications are important for many applications of the mobile ad hoc networks (MANETs) deployed in adversary environments. A major requirement on the network is to provide unidentifiability and unlinkability for mobile nodes and their traffics. The existing protocols are vulnerable to the attacks of fake routing packets or denial-of-service (DoS) broadcasting, even the node identities are protected by pseudonyms. In this paper, we propose a group signature based authentication, to secure the communication and defend the attacks. More specifically, the route request packets are authenticated by a group signature, to defend the potential active attacks without unveiling the node identities.

II. METHODOLOGY

2.1 Group Signature

Group signatures have recently become important for enabling privacy-preserving attestation projects. The signatures are as short as standard RSA signatures with comparable security. Security of group signature (in the random oracle model) is based on the Strong Diffie-Hellman assumption and the Decision Linear assumption in bilinear groups..The program runs a group key agreement protocol at the beginning of every time slot and use the resulting group key as the common parameter and scalable. The more efficient approach is to use a group key agreement protocol in order to agree on the common parameter and group

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 5, May 2015

manager to generate and distribute this starting value. Group Signature scheme has group manager, who is response for adding new members and revoking signature of individual nodes in anonymity are given to a group manager.

2.1 Definitions

Formally, a group signature scheme comprises three algorithms, KeyGen, Sign, and Verify, which behave as follows:

KeyGen(n). This randomized algorithm takes as input a parameter n, the number of members of the group. It outputs a group public key gpk, an n-element vector of user keys gsk = (gsk[1], gsk[2], . . . , gsk[n]), and an n-element vector of user revocation tokens grt, similarly indexed.

Sign(gpk, gsk[i],M). The (randomized) signing algorithm takes as input the group public key gpk, a private key gsk[i], and a message M 2 {0, 1}, and returns a signature.

Verify (gpk,RL, ,M). The verification algorithm takes as input the group public key gpk, a set of revocation tokens RL (whose elements form a subset of the elements of grt), and a purported signature on a message M. It returns either valid or invalid. The latter response can mean either that is not a valid signature, or that the user who generated it has been revoked.

The security scheme is based on the following assumption:

(1) All legal nodes join network during the initial period of Network construction. The first assumption depends on the condition that there not exists any malicious node during the initial period of network construction.

(2) All nodes do not join the network at the same time, But in succession.

In practical case the key can be transported for adding new nodes. There are many secure ways of transporting keys to new nodes.

III. Objectives And Overview Of The Protocol

3.1 Objectives

In this paper, we propose to design a group signature based security protocol approach which attains confidentiality and authentication of packets in ZigBee Network. Privacy and network security is goal, which cannot reduce the performance of network. to resist the active and passive attack, the network itself detecting and eliminating the source of attacks.

3.2 Key distribution

In a ZigBee network, a new node usually needs to join the network, and then obtain key for routing message. It is guaranteed that nodes are organized according to Cluster-Tree relationship. In order to distribute key between each pair of nodes, it is convenient to generate key between the network and new node when a node prepares to join a network.

The main functions of key distribution are as follows:

Key establishment: It is a method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received. The nature of the equipping they require depends on the encryption technique they might use. If they use a code, both will require a copy of the same codebook. If they use a cipher, they will need appropriate keys. If the cipher is a symmetric key cipher, both will need a copy of the same key. If an asymmetric key cipher with the public/private key property, both will need the other's public key.

Key transport : The generated public and private keys must be transported between the nodes.

Frame protection: Management frames such as authentication, de-authentication, association, dissociation, beacons, and probes are used by wireless clients to initiate and tear down sessions for network services. Unlike data traffic, which can be encrypted to provide a level of confidentiality, these frames must be heard and understood by all clients and therefore must be transmitted as open or unencrypted. While these frames cannot be encrypted, they must be protected from forgery to protect the wireless medium from attacks.

Device authorization: To authorize *device means* to register it with the network, so that network will recognize it whenever device sign in. For a node to send and receive data it must be added to the network. Device authorization plays a major role in ID verification. The IEEE ID of authorized device are added to the network.

3.3 Diffie–Hellman key exchange

In 1975, published a cryptographic protocol called the Diffie–Hellman key exchange (D–H) based on concepts developed by Hellman's PhD student Ralph Merkle. The protocol enables users to securely exchange secret keys even if an opponent is monitoring that communication channel. The D–H key exchange protocol, however, does not by itself address authentication (i.e. the problem of being sure of the actual identity of the person or 'entity' at the other end of the communication channel). Authentication is crucial when an

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 5, May 2015

opponent can both monitor and alter messages within the communication channel (aka man-in-the-middle or MITM attacks) and was addressed in the fourth section of the 1976 paper.

3.4 Key transportation methods

There are basically three methods for key transportation to add new nodes securely to a network.

Pre-installation: The keys are placed into device using out of band method, e.g. commissioning tool . The method is used during the initial phase of network construction.

Transport: is where the Trust Center sends the key (securely wherever possible) to the device.

Establishment: is where the device negotiates with the Trust Center and keys are established at either end without being transported

Considering that during the period of discovering PAN and selecting PAN, hand-shake protocol is necessary for node's joining a ZigBee network, we adopted D-H algorithm for key exchange. D-H algorithm allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. Thus we can combine the parameter exchange of D-H algorithm into the hand-shake protocol for node's joining a ZigBee network.

D-H algorithm exchanges four parameters by two handshakes, and joining a ZigBee network also requires two handshakes by means of beacon request frame, beacon frame, associate request frame, and associate response frame. Therefore it is feasible to exchange key parameters by means of two hand-shake protocol. By improving the payload field of related frames, the four parameters of n, g,KA,KB for key exchange are attached into beacon request frame, beacon frame, associate request frame, associate response frame, respectively.

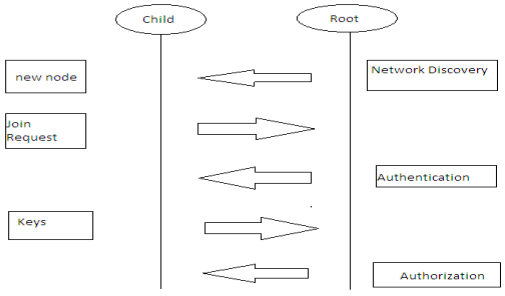

Fig 1.Procedure for joining a network through association

The basic procedure for a new node to join a network is shown in Fig 1. The network discovery detects a new node. Node request to join the network. The root node asks for authorized keys. If the keys are found to be valid then the node is given access to the networks or else rejected.

when node A tries to join ZigBee network by node B, (1) it firstly broadcasts a beacon request frame carrying with parameter n. (2) Node B receiving the beacon request frame generates a large prime number g and broadcasts a beacon frame carrying with parameter g. (3) Node A receives the beacon frame carrying with parameter g and identifies the node address sending the beacon frame. According to the received parameter g, the parameter KA can be calculated. Node A sends a associate request beacon carrying with the parameter KA to node B. (4) Node B receives the associate request beacon, calculates the parameter KB and symmetric key, and then broadcasts a associate response frame carrying with parameter KB. (5) Node A receives the associate response beacon, calculates the symmetric key, and successfully joins the network.

The most serious limitation of Diffie-Hellman in its basic form is the lack of authentication. Communications using Diffie-Hellman all by itself are vulnerable to man in the middle attacks. Ideally, Diffie-Hellman should be used in conjunction with a recognized authentication method such as digital signatures to verify the identities of the users over the public communications medium.

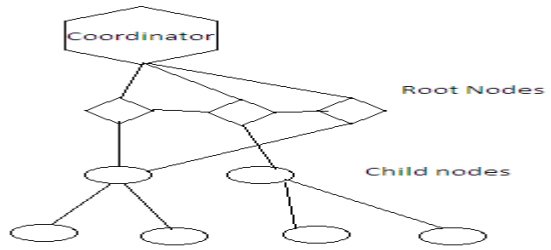

Fig 2.Network Toplogy

The two types of generic 802.15.4 nodes upon which ZigBee devices are based consist of the following:

Reduced Function Devices (RFD): These are reduced complexity nodes with relatively limited memory, processing, and power capabilities. They can only serve as End Devices in a network and cannot perform the more complex roles of Router or Coordinator.

Full Function Devices (FFD)*:* These devices have the resources to perform more complex task such as

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 5, May 2015

Coordinator or Router but can also be an End Device in a network.ZigBee Coordinator*:* Also referred to more generically as the PAN Coordinator, this device is responsible for performing critical functions such as starting a PAN network, assigning device addresses, and controlling the PAN formation and operation. There can be only one Coordinator per ZigBee network, and the Coordinator must be an FFD. ZigBee Router: A Router has the resources to execute routing algorithms and forward message to and from ZigBee devices. It is capable of establishing and maintaining multiple connections to children and parent nodes. A Router must be an FFD. ZigBee End Device *(*ZED*):* An End Device can be an RFD or an FFD but is a leaf node in the network and does not perform any of the other ZigBee device functions of Router, Coordinator, Trust Center, or Gateway. The basic network topology for ZigBee network is shown in fig2. Joining scenario is done after the node has been discovered by the network discovery. Router sends a device update to coordinator for authentication. Coordinator then generates a key encrypt it and transport it to the device. Device retrieves network key from network key transport using pre-configured coordinator link key.

IV. Results And Discussion

One type of passive attacks is a global eavesdropper. As discussed in the previous section, it is impossible for an eavesdropper to obtain the identity information about the source or destination node in any communication..For typical man-in-the-middle attacks, the attacker might completely launch three tasks: (1) obtain the parameter *n* and *g* by sniffing; (2) intercept *K*A and *K*B, then replace them with new *K*_A and *K*_B; (3) calculate *Key*1 by using *K*A and *K*_B, and calculate *Key*2 by using *K*_A and *K*B.The attacks are simulated in the following way: The network takes no action against the attack and the network can detect the malicious node via the group signature, and isolate the attackers in the routing tables.

V. Conclusion

In this paper, we proposed a group signature scheme for secururing ZigBee networks. Group signature is based on the ZigBee hand-shake protocol and improved Diffie-Hellman algorithm with higher security. This can prevent man-in-the-middle attacks during the period of network formation and false routing information attack during the period of route discovery. Despite the performance of network delay might increase, the improved routing protocol necessarily would bring about a better routing security.

In our future work, we will improve algorithm to reduce the packet delay. A possible method is to combine it with a trust based routing. The routing protocols will be more active in detecting link failures, caused either by the mobility or adversary attacks.

References

[1]. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad hoc Networks," in *Proc. IEEE Int'l Conf. Local Computer Networks (LCN'04)*, Nov. 2004, pp. 618–624.

[2]. J. Kong, X. Hong, and M. Gerla, "ANODR: An identity-free and ondemand routing scheme against anonymity threats in mobile ad hoc networks," *IEEE Trans. on Mobile Computing*, vol. 6, no. 8, pp. 888– 902, Aug. 2007.

[3]. K.E.Defraway and G.Tsudik, " Privacy-Preserving Location-based On- Demand Routing in MANETs, " *IEEE Journal on Selecting Areas in Communications*, vol. 29, no. 10, pp. 1926-1934, Dec.2011.

[4]. Hyunjue Kim, JongChung, Chang Hyun Kim, "Secured communication protocol for internetworking zigbee cluster networks", *Computer Communications*, Vol.32, pp.1531–1540, 2009.

[5]. Manel Guerrero Zapata, "Secure Ad hoc on-demand distance vector routing", *Mobile Computing and Communications Review*,Vol.6, No.3, pp.106–107, 2002.

[6]. N. Sastry, D. Wagner, "Security considerations for IEEE 802.15.4 networks", *Proceedings of the 3rd ACM workshop on Wireless security*, Philadelphia, PA, USA, pp.32–42, 2004.

[7]. Satria Mandala, Md. Asri Ngadi and A.Hanan Abdullah, "*A Survey on MANET Intrusion Detection*" IJCSS, Vol No 2, Issue 1, 2007

[8]. Yi .P, Iwayemi .A, and Zhou .C, "Developing ZIGBEE Deployment Guideline under WiFi Interference for Smart Grid Applications," IEEE Trans. Smart Grid, vol. 2, no. 1, pp. 110-120, Nov. 2011.

[9]. Vani A and Rao D, "*Providing of Secure Routing against Attacks in MANETs*" International Journal of Computer Applications (0975 – 8887) Volume 24– No.8, June 2011.

[10]. Wei Liu and Ming Yu, "AASR:Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments," *IEEE Transaction On Vehicular Technology.*, vol. X, no. Y, May 2014.

[11]. Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in *Proc. IEEE INFOCOM 2005*, vol. 3, Mar. 2005, pp. 1940–1951.

[12]. Zheiong Wei, Helen Tang, F.Richard Yu, Maoyu Wang and Peter Mason, " Security Enhancements for Mobile Ad hoc Networks with Trust Management Using Uncertain Reasoning, " *IEEE Transaction On Vehicular Technology*, vol. X, no. Y pp. 1-12, 2013.