International Journal of Computer Science and Informatics

Volume 4 | Issue 2 Article 12

October 2014

COMPARATIVE STUDY OF MULTI USER BROADCAST AUTHENTICATION IN WIRELESS SENSOR NETWORK

P. PRASUNA
Keshav Memorial Institute of Technology, p.prasuna@gmail.com

COMPARATIVE STUDY OF MULTI USER BROADCAST AUTHENTICATION IN WIRELESS SENSOR NETWORK

P. PRASUNA[1], DR. R.HEMALATHA[2]

[1]Keshav Memorial Institute of Technology, [2]College of Engineering Osmania University

Abstract- Wireless sensor network (WSN) is an emerging technology consisting of spatially distributed sensor nodes, which can cooperatively monitor physical or environmental conditions. The major resource constrain of WSN are, low processing, energy and storage capabilities. Broadcast is widely used communication method in WSN environment. In most of the sensor networks, the sink node sends broadcast information to all other sensor nodes. Broadcast authentication is an important security mechanism in WSN, as it allows mobile users to broadcast messages to multiple sensor nodes in a secured way. While variety of multiuser broadcast authentication approaches are being developed, a lot of research is going on in the security field at rapid pace. However this field lacks a common integrated platform to provide a comprehensive comparison of seemingly unconnected but linked issues .In this article a pilot survey is performed to classify the, already proposed multiuser broadcast authentication approaches. This comparative survey is based on the objective, design principles and the performance of multiuser broadcast authentication approaches

Keywords- *Wireless sensor network (WSN), Broadcast communication, authentication, Distributed sensors, Multiuser.*

1. INTRODUCTION:

The development of WSN and its application in industries such as health care, consumer and military have attracted much research to develop protocols and algorithms related to WSN. The research issues in WSN application can be categorized based on networking, topology, security, authentication, communication of data between nodes and motes and so on. Typically any WSN consists of sensor nodes which are wirelessly networked to each other. These groups of sensor nodes are in turn controlled by individual base stations as shown in figure 1.1 which are resource limited devices with low processing, energy and storage capabilities.

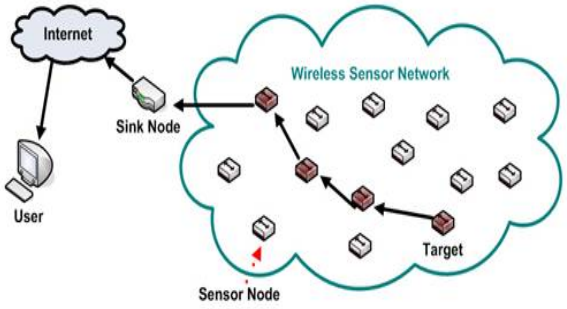

Fig 1.1 Wireless sensor network (WSN)[10]

In the process of data communication between nodes, the major role of an individual sensor node is to transmit its messages first to the base station using unicasting technique from where these messages are broadcasted to other sensor nodes. Broadcasting of a message between nodes requires certain authentication procedure to sustain security mechanism in WSN. Several broadcast authentication protocols have been proposed for WSN, out of which the two major protocols considered in this survey are symmetric cryptography schemes which are MAC(Message authentication code) based as shown in figure 1.2

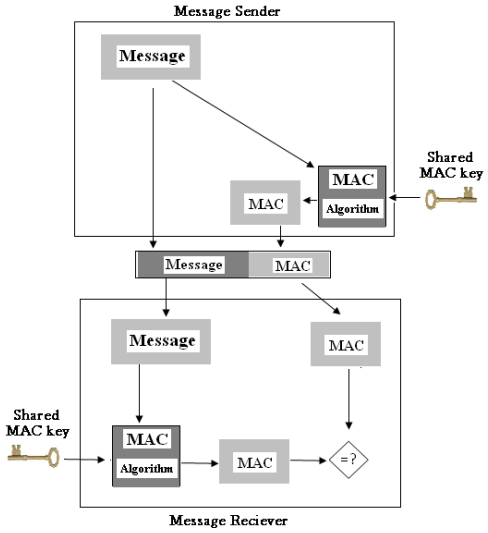

Fig 1.2 MAC based symmetric protocol

The asymmetric cryptography scheme based on digital signature concept as shown in figure 1.3

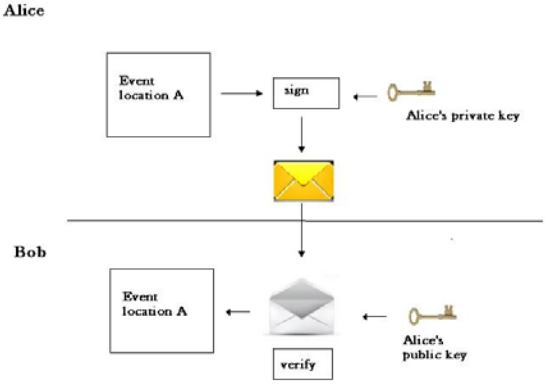

Fig 1.3 Digital signature based asymmetric protocol

2. SCHEMES BASED ON SYMMETRIC CRYPTOGRAPY:

A typical pair wise MAC is a conventional symmetric approach in WSN authentication, but cannot be employed for the broadcast setting in WSN due to the presence of compromised nodes in network.

µ Tesla was the first approach that addressed the broadcast authentication problems in WSN [1]. Based on the type of sender symmetric authentication can be categorized as

I. Resourceful sender
II. Resource constrained sender

2.1 RESOURCEFUL BROADCAST SENDER SCHEMES:

This broadcast authentication schemes assumes resourceful devices as senders and resource constrained sensor nodes as receivers. It employs a MAC key with a delay disclosure which helps to avoid attacks launched by compromised sensor nodes. At the initial point of broadcast among receivers, MAC key is not shared whereas after a delay the MAC key is sent to all broadcast receivers for authentication. MAC key of µ Tesla involve multiple phases such as sender setup, broadcast authentication packets, bootstrapping new receivers etc. µ Tesla suffers from major problems like distribution of key chain, slow authentication and Dos (denial of service) attack. It is not suited for large scale WSN.

Multilevel µ Tesla deals with handling problems related to distribution of new chain commitments [2]. Its basic concept is to prolong the life of broadcasting without storing long key chains and to authentically distribute new key chain commitments to the receivers. This scheme involves two different levels of key chain to authenticate broadcast message from base station and high level key chain. The major problem associated with this scheme is delayed authentication and scalability in terms of number of sensor nodes.

Multi sender µ Tesla scheme provides scalability in terms of number of broadcast sender [3]. It involves concept of dividing time period among multiple senders instead of single broadcast sender, thus base station transmits message one by one in their allotted time intervals. Major limitation of this scheme is, it does not allow multiple senders to broadcast at the same time. Each sender is allowed to transmit message at a predefined fixed time interval thus it is not suited for real time applications.

L-tesla scheme decrease the delay in message authentication for large scale sensor networks [4]. It divides the sensor node network into equal subsets and parallely authenticates single message in these subsets. It relies on trusted nodes in the network which are secured with more computing and communication capabilities. This scheme is not suitable for unevenly distributed network and also suffers in the absence of trusted nodes.

2.2 SCHEMES WITH RESOURCE CONSTRAINED BROADCAST SENDER:

This scheme assumes resource constrained sensor nodes as broadcast sender as well as receiver. Multilevel µ Tesla is the mechanism involved in which sensor nodes distribute key chain commitments only to the nearby sensor node. This mechanism suffer with major drawbacks such as limited storage, difficulty in identifying of neighboring nodes, limitation in number of broadcast senders and receivers. Bootstrapping key chain commitment may reduce the problem to a certain extent.

Multiuser broadcast authentication schemes discussed based on µ Tesla mechanism exhibit certain flaws such as delayed authentication, consumption of time, lack of scalability, Dos attacks, it also has problem with time slot allocation, key chain distribution etc. Hence the following section reviews schemes based on asymmetric cryptography which addresses several limitation of µ Tesla mechanism.

3. SCHEMES BASED ON ASYMMETRIC CRYPTOGRAPHY:

Concept of this scheme is that it assumes resourceful devices as broadcast sender and not typical sensor nodes. It uses public key cryptography (PKC) based digital signature method where message signer signs a message using his private key and receiver verifies the signed message using a public key.

CAS (certificate based authentication scheme) contains a certificate with the public key of broadcast sender, signed by the private key of a fixed base station [5][6]. The sender uses private key to sign the message and broadcast the message along with certificate to other nodes. The receiver node verifies the signed certificate using public key and if it succeeds, verifies signed message from public key. DAS (Direct storage base authentication scheme) ensures that every receiver stores ID's and respective public keys of all broadcast senders. Now a broadcast sender uses a private key to sign the message and broadcast it with its ID's and public key pair. The receiver verifies for ID and public key pair. If satisfied, receiver further verifies the signed message using public key. Major limitation of DAS and CAS schemes is increase in computation and storage overhead due to additional usage of public and private key in broadcast authentication process.

Merkly hash tree suggested MAS (Merkly hash tree authentication scheme) to avoid the storage overhead

of DAS [7]. Each node has a hash value of broadcast sender and receiver stores the value of root node to authenticate public keys of broadcast sender. The major flaw of this approach is, it is not dynamic but the message size can be increased especially for large scale sensor node. Another approach based on BAS (Bloom filter based authentication scheme) use the bloom filter to store public key [5]. Unlike DAS and BAS, this scheme does not preload the sensor node with ID and public key of base station. Instead each sensor node stores hash mapping of ID and public key pairs. Using bloom filter when sensor node receives message with ID and public key pair, it checks authenticity using hash mapping stored in memory.

HAS (Hybrid authentication scheme) approach combines BAS and MAS to reduce message length and storage space and thus enhances scalability. At the cost of increase in message size HAS can support more broadcast senders than BAS. Asymmetric based authentication discussed so far mainly adapts the management of public key and certificate in WSNs. ECDSA(Elliptic curve digital signature algorithm) and RSA(Ron Rivest Adi Shamir algorithm) are the two techniques widely employed to solve problem of public keys and certificate management. [8][9]

CONCLUSION:

Security in wireless sensor network has attracted many researches due to its unique environment orientation. All the symmetric and asymmetric cryptography based authentication schemes that have been presented in this paper suffer from significant limitations. In case of symmetric schemes, the limitations are it requires regular and predefined interval broadcasting, storage of μ Tesla parameters, the distribution of key chain commitments and the delayed authentication. μ Tesla based schemes fail to provide a solution to real time application of WSNs and scalability. In case of asymmetric schemes limitation are the management of public keys and certificate. The cost of applying PKC on sensor nodes particularly is more time consuming and critical for real time application. Various schemes for ensuring broadcast authentication in WSNs have been surveyed and investigated, based on time consumption and scalability. This paper gives a broad idea in selecting broadcast authentication protocols to suit the need of the researcher.

REFERENCES:

[1]. Perrig, Robert Szewczyk, J.D.Tygar, VictorWen, andDavid E. Culler. SPINS: Security Protocol for Sensor Networks. Wireless Networks, 8(5):521-534, 2002

[2]. Donggang Liu and Peng Ning. Multilevel μ Tesla: Broadcast authentication for distributed sensor networks. ACM Transaction on Embedded computing systems (TECS), 3(4):800-836, 2004

[3]. Donggang Liu, Peng Ning, Sencun Zhu and Sushil Jajodia. Practical broadcast authentication in sensor networks. In Proceedings of MobiQuitous ’05: Networking and Services, pages 118-132.IEEE Computer Society, 2005.

[4]. Jawed Drissi and Qijun Gu. Localized broadcast authentication in large sensor networks. In Proceeding of International conference on Networking and services- ICNS ’06, pages 25.IEEE, 2006.

[5]. Kui Ren Wenjing Lou, and Yanchao Zhang. Multi-user broadcast authentication in wireless sensor networks. In Proceeding of sensor, Meshand Adhoc communication and Networks-SECON ’07, pages 223-232, 2007.

[6]. Kui Ren, Wenjing Lou, Kai Zeng, and P.J Moran. On broadcast authentication in wireless sensor network. Wireless Communication, IEEE Transactions on 6(11):4136-4144, 2007

[7]. Ralph C.Merkle. Protocols for public key cryptosystem. In IEEE Symposium on security and Privacy, pages 122-134, 1980.

[8]. Don Johnson, Alfred Menezes, and Scott A. Vanstone. The elliptic curve digital signature algorithm (ECDSA). International Journal of Information Security,1(1):36-63, 2001.

[9]. Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signature and public-key cryptosystem. Communication, ACM, 21(2):120-126, 1983.

[10]. http://monet.postech.ac.kr/images/introduction/image007.jpg

◈◈◈