

An ID Based Aggregate Scheme for Multiuser Broadcast Authentication in Wireless Sensor Networks

Hemavathy. R¹ Keerthana. V² Kirthana. P³ Dr B. Jaison.⁴

^{1,2,3}Student ⁴Associate Professor

^{1,2,3,4}Department of Computer Science & Engineering

^{1,2,3,4}R.M.K Engineering College, Chennai, India

Abstract— Multiuser Broadcast authentication plays a vital role in Wireless Sensor Networks (WSN) as it allows a large number of users of WSN's to broadcast and receive messages from many sensor nodes securely. Many schemes like symmetric key cryptography, Public key Infrastructure (PKI) have been proposed to implement broadcast authentication to users in wireless sensor networks, but these schemes have few disadvantages like high energy consumption due to wireless transmission of messages, high cost of public key certificates and energy depletion of sensors due to continuous monitoring. This paper proposes solutions for the energy consumption of each sensor and multiuser broadcast authentication based on the email id of the user.

Key words: Broadcast Authentication, Sink, User and Sensor

I. INTRODUCTION

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes. A WSN is composed of two types of nodes: sink nodes and sensor nodes. A sensor is a small device that has a micro sensor capability, low power, signal processing, low power computation and a short range communications capability. While sensor nodes collect surrounding information with sensors, a sink node is in charge of connection between the Internet and sensor nodes. A sink node plays an important role as a gateway, so it has powerful and redundant components for the high reliability. The sink acts as an authority for all the sensor nodes in the network. On the other hand, sensor nodes are typically equipped with low-end components in consideration of cost, because generally hundreds of or thousands of sensor nodes are needed for a WSN to provide the secure monitoring function. These sensor nodes are able to sense or monitor the world entity. They are in charge of collecting data and routing this information back to a sink. Many sensors keep sending data periodically to one base station making it a many to one communication scenario. The traditional way of broadcast in WSN is flooding, which is the straightforward and obvious way. When a source node has a packet to broadcast in the network, it sends the packet to all of its neighbors. Then each node that has received the packet for the first time will rebroadcast the packet to its neighborhood, which leads to the participation of all the nodes in broadcasting the packet. Thus, the traditional flooding which also is known as ordinary broadcast mechanism (OBM), results in serious redundancy, collision and contention, and referred to as broadcast storm. Initially, the sensor nodes are preloaded

with $K_0 = hn(x)$, where x is the secret held by the sink. Then, $K_1 = hn^{-1}(x)$ is used to generate MACs for all the broadcast messages sent within time interval I_1 . During time interval I_2 , the sink broadcasts K_1 , and the sensor nodes verify $h(K_1) = K_0$. The authenticity of messages received during time interval I_1 is then verified using K_1 . This delayed disclosure technique is used for the entire hash chain and thus leads to loosely synchronized clocks between the sink and sensor nodes. In Wireless Sensor Networks there would be the large number of user in the network they can join the network dynamically, so proper multi user authentication is required in order to prevent attacker those can able to modify the information or providing false information in the network.

II. PRELIMINARIES

Symmetric key schemes are not viable for mobile sensor nodes and thus past approaches have focused only on static WSNs. A few approaches have been proposed based on PKC to support dynamic WSNs. Thus, in this section, we review previous PKC-based key management schemes for dynamic WSNs and analyze their security weaknesses or disadvantages. The first existing system adopts a one-way hash function $h()$ for broadcast authentication and message authentication code (MAC) algorithm. The hash function uses a string of arbitrary length as its input and creates a fixed-length string as output. The fixed-length hash value is often called message digest. The most widely used hash functions are one-way functions for which finding an input which hashes to a pre-specified hash-value is very difficult. But these would provide several active attack due to the propagation delayed of disclosed key and delayed authentication of broadcast message. Public key cryptography (PKC) solves these problems, i.e it provides flexible functionalities without the need for key pre-distribution and pair wise key sharing. PKC is feasible to small wireless device with limited resources. PKCs need to authenticate users' public keys, it utilizes Public-key infrastructure (PKI). PKI is an arrangement that binds public keys with respective users' identities by means of public-key certificates issued by a Certificate Authority (CA). The public-key certificate contains a user's public key and CA's signature on the public key. Since a WSN adopts flooding mechanism in practical broadcast and the data rate in WSN is restricted, the message transmission is always energy-consuming. Thus, the use of public-key certificates consumes substantial bandwidth and power due to the transmission and verification of the certificates, since wireless transmission is very expensive. The limited computation and power resources of sensor nodes often makes it undesirable to use public-key algorithms, a sensor node may require on the order of tens of seconds up to

minutes to perform these operations This exposes a vulnerability to denial of service (DoS) attack. The amount of key-storage memory in a given node is highly constrained; it does not possess the resources to establish unique keys with every one of the other nodes in the network.

III. SYSTEM MODEL & NETWORK MODEL

A. SYSTEM MODEL

In this paper, we consider a large spatially distributed WSN consisting of a fixed sink(s) and a large number of sensor nodes. The sensor nodes are usually resource constrained with respect to memory space, computation capability, bandwidth, and power supply. The WSN is aimed to offer information services to many network users that roam in the network, in addition to the fixed sink(s).

B. NETWORK MODEL

A WSN consists of a large number of resource-constrained sensor nodes, many sensor network users, and a single network owner. The network users (e.g., soldiers) use mobile devices such as personal digital assistants (PDAs) or laptop PCs to reprogram the sensor nodes. The network users may include mobile sinks, vehicles, and people with mobile clients, and they are assumed to be more powerful than sensor nodes in terms of computation and communication abilities. For example, the network users could consist of a number of doctors, nurses, medical equipment (acting as actuators), and so on, in the case of Code Blue, where the WSN is used for emergency medical response. The network owner can be offline, who has bootstrapped the keying materials for the mobile devices to enforce reprogramming privilege policy. It is assumed that the network owner cannot be compromised and has unlimited computational power compared with sensor nodes. Such sensor networks are under construction or planning by many multi sponsor programs and projects. We assume that the sink is always trustworthy, but the sensor nodes are subject to compromise. At the same time, the users of the WSN may dynamically be revoked due to either membership changes or compromise, and the revocation pattern is not restricted. We also assume that the WSN is loosely synchronized. The sensor nodes can only perform a limited number of asymmetric cryptographic operations, such as signature verification, due to the large energy consumption of these operations. We also assume that sensor nodes are able to establish pair wise keys between neighbour nodes-assorted military services.

IV. PROPOSED SYSTEM

In this paper, we propose Identity (ID)-based infrastructure which allows a user's public key to be easily computed from its known identity information and thus eliminates the need for public-key Certificates, It has been applied to solve the problems of PKI technology. Broadcast Authentication can be achieved based on ID Based Signature scheme from pairing free (Fig:1). We utilize pairing free signature schemes with message recovery in the ID-based infrastructure, which is probably secure in the formal security model.

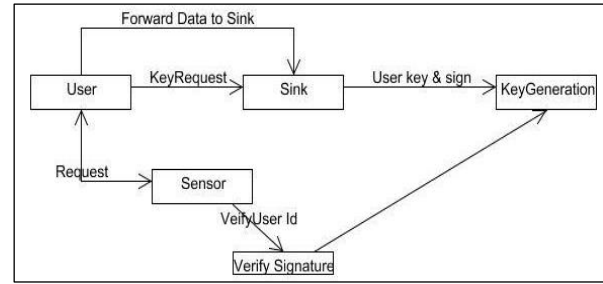


Fig: 1

V. MODULES

- 1) Network Formation
- 2) User Authentication for Sending request
- 3) Sensor sending information to user
- 4) User forward to sink and user revoke

A. Network Formation:

First we create the sink (Base station), this sink acts as the main authority for providing keys to the user. The user in this context refers to those working in Military, Disaster and the Detection, Environmental Monitoring etc domains. The sink will continuously monitor the user as well as the sensor and it is responsible for providing public and private key for the user and for authenticating the user based on signature. Then the user is created based on the distance and range within which the sensor is present. In this paper we have proposed to keep the range should be less than the distance. This distance and range will be calculated to determine the coverage of an individual user. Later, the user requests the sink to generate keys, the sink provides the user with one public key and private key based on the user's email id. Then sensor will be created with distance and range, here sensor will sense the Temperature and Humidity.

B. User Authentication for Sending Request:

In wireless sensor networks, the Sink and the user are the most powerful entities than the sensor. User is responsible for sending the data to the sink before sending any information to the particular user. So in this scenario user authentication is needed in order to prevent the false user in the network. User will send the query to the sensor to get information like temperature or the humidity. Once the request received by the sink, it should verify that he is the authenticate user in the network by verifying the signature. If the user is valid user then he can able to send the request to sensor for information. User can send the request to the sensor that comes in the user coverage area.

C. Sensor sending information to user

If the user signature is matched, then he can able to send the request to the sensor those are comes within the coverage range with any query like temperature or humidity. The sensor then sends the data to the user based on which the user has asked the request. Sensor will send the content in the encrypted format. Sensor will encrypt the content based on user identity, for decrypt the content user need to verify his secret key and mail it and decrypt the content and get the original content.

D. User forward to sink and revoke

In this network, sensor will not send any message directly to sink, user is responsible for sending the information to the sink in order to save the energy of sensor. Sensor has not much energy to sense and to transmit the information directly to sink. So sensor will sense and send the information to the authorized user, user will send the information to the sink. Sink again check the user authentication if user has sent the proper and correct information, then the user is trusted or else sink will revoke the user and inform to all the sensor. Later when the sensor received the request from the revoke user directly then drop the request. In this paper, we have proposed a solution where each sensor take turns for monitoring. When a sensor is monitoring, the remaining sensors remain idle. By this way the energy of each sensor gets consumed effectively. Below are the images which depict the sensor monitoring the temperature and humidity. The red colour indicates currently the sensor is monitoring while grey colour indicates that the sensor is idle.



VI. CONCLUSION

Thus, Multiuser is been authenticate without much delayed for providing the key, & user authentication in verified by the authority and the communication overload between the sensor and sink is reduce and energy of an individual sensor is saved.

REFERENCES

- [1] Kui Ren, Kui Ren, Wenjing Lou, Wenjing Lou, Yanchao Zhang, and Yanchao Zhang. Multi-user broadcast authentication in wireless sensor networks. In SECON'07 4th Sensor, Mesh and Ad Hoc Communications and Networks, pages 223–232, 2007.
- [2] K. Ren, W. Lou, and Y. Zhang, “Multi-user broadcast authentication in wireless sensor networks,” in Proc. SECON, San Diego, CA, Jun. 2007, pp. 223–232.
- [3] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz, “Energy analysis of public-key cryptography on small wireless devices,” in Proc. IEEE PerCom, Kauai, HI, Mar. 2005, pp. 324–328.
- [4] W. Du, R. Wang, and P. Ning, “An efficient scheme for authenticating public keys in sensor networks,” in Proc. MobiHoc, Urbana-Champaign, IL, May 2005, pp.58–67.
- [5] W. Du, J. Deng, Y. Han, and P. Varshney, “A pairwise key predistribution scheme for wireless sensor networks,” in ACM CCS, Washington, DC, Oct. 2003.
- [6] W. Du, J. Deng, Y. Han, S. Chen, and P.K.Varshney, .A key management scheme for wireless sensor networks

- using deployment knowledge,. In IEEE INFOCOM, HongKong, China, March 2004.
- [7] M. Rahman and K. El-Khatib, “Private key agreement and secure communication for heterogeneous sensor networks,” J. Parallel Distrib. Comput., vol. 70, no. 8, pp. 858–870, 2010.
- [8] G. Gaubatz and B. S. J. Kaps, “Public keys cryptography in sensor networks – revisited,” in ESAS'04, EURESCOM, Heidelberg, Germany, Aug. 2004.
- [9] X. He, M. Niedermeier, and H. de Meer, “Dynamic key management in wireless sensor networks: A survey,” J. Netw. Comput. Appl., vol. 36, no. 2, pp. 611–622, 2013.
- [10] Y. Zhou, Y. Zhang, and Y. Fang, “LLK: a link-layer key establishment scheme in wireless sensor networks,” in IEEE WCNC'05, New Orleans, LA, Mar. 2005.
- [11] L. Eschenauer and V. Gligor, “A key-management scheme for distributed sensor networks,” in ACM CCS, Washington, DC, Nov. 2002.
- [12] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in IEEE Symposium on Security & Privacy, Oakland, CA, May 2003.
- [13] D. Liu and P. Ning, “Establishing pairwise keys in distributed sensor networks,” in ACM CCS, Washington, DC, Oct. 2003.
- [14] D. Du, H. Xiong, and H. Wang, “An efficient key management scheme for wireless sensor networks,” Int. J. Distrib. Sensor Netw., vol. 2012, Sep. 2012, Art. ID 406254.
- [15] Ren, K., S. Yu, W. Lou and Y. Zhang, 2009. “Multi-User Broadcast Authentication in Wireless Sensor Networks”, IEEE Transactions on Vehicular Technology, Vol. 58, No. 8.
- [16] D. Liu and P. Ning, .Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks,. in Proc.NDSS'03, San Diego, CA, Feb. 2003.
- [17] W. Lee and W. Sriborrirux, “Optimizing authentication mechanisms using ID-based cryptography in ad hoc wireless mobile networks,” in Int. Conf. Inform. Netw. - ICOIN'04, ser. Lecture Notes in Computer Science, H.-K. Kahng and S. Goto, Eds., vol. 3090. Berlin: Springer-Verlag, Feb. 2004, pp. 925–934.