Research Paper Engineering

PKC Based Broadcast Authentication Scheme for Identifying Misbehaving Forwarders and Intruders in Wireless Sensor Networks

*T.P.Udhaya Sankar **Dr.S.Vijayaragavan ***K.Banupriya

* Assistant Professor /Computer Science and Engineering, Annapoorana Engineering College, Salem

** Professor & Center Head,Paavai Engineering College, Pachal, Namakkal

*** M.E. Computer Science and Engineering,Paavai Engineering College, Salem

ABSTRACT

Broadcast authentication is a critical security service in wireless sensor networks (WSNs) which allows the mobile users to broadcast messages between multiple sensor nodes in a secure way. To defend the WSNs against the adversary attacks will inject malicious traffic to reduce the energy from the sensors that the broadcast authentication of source and receivers becomes extremely unavoidable. Public Key Cryptography (PKC) is widely used for broadcast authentication. Intensive use of PKC for broadcast authentication is to be expensive to resource constrained sensor nodes. The system proposes a novel PKC based broadcast authentication scheme using signature amortization for Wireless Sensor Networks (WSNs). The proposed scheme exploits only one Elliptic Curve Digital Signature Algorithm (ECDSA) signature to authenticate all broadcast messages. Thus, the overhead for the signature is amortized over all broadcast messages. Besides low overhead, the proposed scheme retains high security that is as strong as conventional PKC based broadcast authentication schemes.

Keywords : Packet Dropping, Packet Modification, Intrusion Detection, Wireless Sensor Networks, PKC, EDSCA, Distributed Key Generation Scheme.

I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of one or more powerful base stations and hundreds of sensor nodes. Base stations serve as gateways between Internet users and sensor nodes. Sensor nodes integrated with microcontroller, Radio Frequency (RF) transceivers and sensing units are spatially scattered into a specific area and monitor physical and environmental conditions. In WSNs, broadcast transmission is one of the fundamental communication primitives[1]. There are two kinds of broadcast transmissions. One is the network broadcast, which may be used by a base station for committing network queries and broadcast code images. The other is the local broadcast, which may be used for discovering neighbors and exchange routing information. Eavesdropping on the unidirectional broadcast transmission, an adversary is able to intercept broadcast messages, change the intercepted messages on behalf of it and rebroadcast them. Even, the adversary may fabricate messages and inject them to the network. These malicious messages may cause crash of sensor nodes or destruction of the entire network. To defend WSNs against malicious messages, it is necessary to authenticate broadcast messages, referred to as broadcast authentication.

Providing broadcast authentication for WSNs encounters many challenges [2]. The primary one is stringent resource constraints on sensor nodes. It results in conventional Public Key Cryptography (PKC) based broadcast authentication schemes are believed to be too expensive for WSNs. For instance, it takes 14 seconds for an exponential operation of 1024-bit RSA on Mica1 motes. Besides resource constraints, sensor nodes are vulnerable to node compromise attacks. This renders application of conventional symmetric key cryptography based broadcast authentication schemes to WSNs impractical.

II. SYSTEM DESCRIPTION

For simplicity, consider only the case of one base station within a WSN. Since WSNs are generally composed of a collection of base stations and sensor nodes are connected to them, the proposed scheme can also be implemented with a WSN having multiple base stations. Assume that there is only one base station that is endowed with sufficient energy supply. Furthermore, it cannot be compromised by adversaries, which is a common assumption in the literature of WSNs (e.g., [20]). Contrary to the base station, sensor nodes are resource constrained and vulnerable to adversaries. Assume that a senor node is able to perform a limited number of PKC operations but not many. In the WSN, both the network broadcast and the local broadcast are considered. For clarity, consider that one sender broadcasts messages to many receivers. In the network with multiple senders, each sender and its corresponding receivers are just the cases are considering. The sender may be the base station or a sensor node.

III. EXISTING WORK

Packet dropping and modification are common attacks that can be launched by an adversary to disrupt communication in wireless multi hop sensor networks. Many schemes have been proposed to mitigate or tolerate such attacks, but very few can effectively and efficiently identify the intruders [1]. To address this problem, propose a simple yet effective scheme, which can identify misbehaving forwarders that drop or modify packets. Extensive analysis and simulations have been conducted to verify the effectiveness and efficiency of the scheme.

All sensor nodes form a DAG and extract a routing tree from the DAG. The sink knows the DAG and the routing tree, and shares a unique key with each node. When a node wants to send out a packet, it attaches to the packet a sequence number, encrypts the packet only with the key shared with the sink, and then forwards the packet to its parent on the routing tree. When an innocent intermediate node receives a packet, it attaches a few bits to the packet to mark the forwarding path of

the packet, encrypts the packet, and then forwards the packet to its parent. As the tree structure dynamically changes every time interval, behaviors of sensor nodes can be observed in a large variety of scenarios. On the contrary, a misbehaving intermediate node may drop a packet it receives. On receiving a packet, the sink decrypts it, and thus finds out the original sender and the packet sequence number. The sink tracks the sequence numbers of received packets for every node, and for every certain time interval, which will call a round, it calculates the packet dropping ratio for every node. Based on the dropping ratio and the knowledge of the topology, the sink identifies packet droppers based on rules will derive.

IV. PROPOSED WORK

Public Key Cryptography (PKC) is widely used for broadcast authentication. Intensive use of PKC for broadcast authentication is idea to be expensive to resource constrained sensor nodes that proposes a novel PKC based broadcast authentication scheme using signature amortization for Wireless Sensor Networks (WSNs). The proposed scheme exploits only one Elliptic Curve Digital Signature Algorithm (ECDSA) signature to authenticate all broadcast messages. Thus, the overhead for the signature is amortized over all broadcast messages. Besides low overhead, the proposed scheme retains high security that is as strong as conventional PKC based broadcast authentication schemes. [3]. Secret sharing allows a secret to be shared among a group of users (also called shareholders) in such a way that no single user can deduce the secret from his share alone. This scheme is to share polynomials in such a manner that the coefficients of the polynomial would always remain secret. A distributed pairwise key establishment scheme based on the concept of bivariate polynomials. Any mobile node in an ad hoc network can securely communicate with other nodes just by knowing their corresponding IDs.

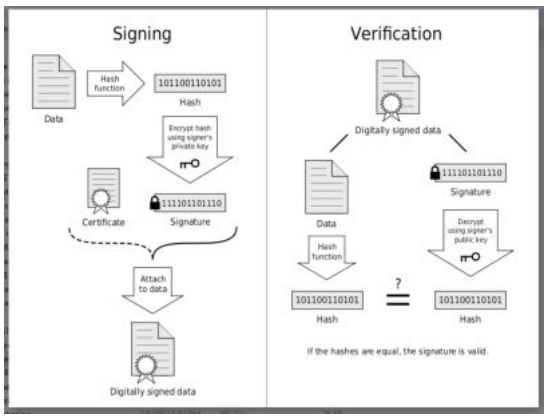

Fig. 1. System Architecture

Before a sender can use digital signing, she must obtain a key pair produced for that purpose. This key pair, consisting of a public key and a private key, can be created by the sender's employer or obtained from a Certificate Authority (CA). The value of the key pair lasts as long as the private key remains private. Key management is beyond the scope of this entry, but is a very important part of not only digital signature deployment. It's also critical to the success of any certificate or key-based security infrastructure.

Once the sender is issued a key pair, the process depicted in Figure 1 is followed to sign and ensure the integrity of messages. The message to be signed is processed by a hash algorithm. The resulting hash value is used to check if the message content changes after the message is sent. This is the step that begins the message integrity checking process.

1. The sender's hash value is encrypted using the sender's private key. This constitutes the sender's digital signature. The assumption is made that no one else has access to the sender's private key.
2. The encrypted hash value is attached to the message, and the message is sent.
3. The message is separated from the encrypted hash.
4. The receiving system decrypts the sender's hash value using the sender's public key. The person receiving the message must obtain the public key from either the sender or a public key repository.
5. The message is processed by a hash function similar to the sender's.
6. The sender's unencrypted hash value and the receiver's hash value are compared. If they're the same, message integrity and the sender's identity are assured; the signature is valid.

V. IMPLEMENTATION AND EXPERIMENTAL RESULTS

We conduct experiments on a multi-hop testbed consisting of TelosB sensor nodes. Using the testbed, we study the performance of the proposed scheme. For simplicity, we have considered a multi-hop testbed consisting of several sensor nodes. Since this is a small set of a real life WSN, we believe that our experimental results can also be applied to the network with hundreds of sensor nodes. For comparison, we also implement a message oriented signature scheme which represents conventional PKC based broadcast authentication schemes and HMAC which represents conventional symmetric key cryptography based broadcast authentication schemes.

VI. CONCLUSION

Many WSN applications require communication between the sensor nodes to be secure and free from attacks by malicious nodes. A novel PKC based broadcast authentication scheme using signature amortization for WSNs is achieved from the proposed protocol that secures communication by distributing the public key securely. The public key that is broadcast, can be retrieved only by the regular nodes, where as malicious nodes cannot. The proposed scheme employs only one ECDSA signature to authenticate all broadcast messages. The overhead of the signature is amortized over all broadcast messages. Besides low overhead, the proposed scheme retains high security as strong as conventional PKC based broadcast authentication schemes. Moreover, the proposed scheme overcomes defects of μTESLA, that is, it does not require time synchronization, has an efficient public key distribution protocol and can achieve immediate authentication. Experimental results show that the overhead of the proposed scheme is to the same degree of HMAC.

The idea of the distributed key generation scheme can also be extended to provide a hierarchical key generation mechanism based on the level of trust that a node wishes to provide to another node. Although we have not developed this idea, it can provide grounds for future work.

REFERENCES

[1] C. Wang, T. Feng, J. Kim, G. Wang,"Catching Packet Droppers and modifiers in Wireless sensor Networks,"IEEE Transactions on Parallel and Distributed Systems, vol.23, no.5, pp.835-843, may 2012. | [2] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003. | [3] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE First Int'l Workshop Sensor Network Protocols and Applications, 2003. | [4] V. Bhuse, A. Gupta, and L. Lilien, "DPDSN: Detection of Packet- Dropping Attacks for Wireless Sensor Networks," Proc. Fourth Trusted Internet Workshop, 2005. | [5] M. Kefayati, H.R. Rabiee, S.G. Miremadi, and A. Khonsari "Misbehavior Resilient Multi-Path Data Transmission in Mobile Ad-Hoc Networks," Proc. Fourth ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '06), 2006. | [6] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, "Secmr—A Secure Multipath Routing Protocol for Ad Hoc Networks," Ad Hoc Networks, vol. 5, no. 1, pp. 87-99, 2007. | [7] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM, 2004. | [8] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by- Hop Authentication Scheme for Filtering False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004. | [9] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward Resilient Security in Wireless Sensor Networks," Proc. Sixth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc '05), 2005. | [10] Z. Yu and Y. Guan, "A Dynamic En-route Scheme for Filtering False Data in Wireless Sensor Networks," Proc. IEEE INFOCOM, 2006. |