OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Security in Wireless Sensor Networks Using Broadcasting

Sneh Lata[1], Sandeep Gupta[2]
[1,2]Hindu College of Engineering

ABSTRACT: *Wireless sensor networks as one of the growing technology in the coming decades has posed various unique challenges to researchers. A WSN typically consists of several base stations and thousands of sensor nodes, which are resource limited devices with low processing, energy, and storage capabilities.While the set of challenges in sensor networks are diverse, we focus on security of Wireless Sensor Network in this paper. As today's world is growing more towards the Wireless technology, our aim must be towards providing the best security features to Wireless Sensor Network(WSN).We propose some of the security requirements for Wireless Sensor Network. Further, security being vital to the acceptance and use of sensor networks for many applications. We propose an efficient broadcast authentication scheme for wireless sensor networks in this paper.*

Keywords: *Broadcast, security, sensors, Wireless sensor network(WSN).*

I. INTRODUCTION

A sensor is a device that translates parameters or events in the physical world into signals that can be measured and analyzed. Sensor networks refer to a heterogeneous system combining tiny sensors and actuators with general purpose computing elements.Wireless Sensor Networks are diverse due to the availability of micro-sensors and low-power wireless communications. Unlike the traditional sensors, in the remote sensor network, a vast numbers of sensors are densely deployed. These sensor nodes will perform significant signal processing, computation and network self-configuration to achieve scalable, robust and long-lived networks.Broadcast is an important communication primitive in wireless sensor networks. It is highly desirable to broadcast commands and data to the sensor nodes due to the large number of sensor nodes and the broadcast nature of wireless communication. Due to the limited signal range, it is usually necessary to have some receivers of a broadcast packet forward it in order to propagate the packet throughout the network (e.g., through flooding, or probabilistic broadcasting). Broadcast authentication is a basic and important security mechanism in a WSN because broadcast is a natural communication method in a wireless environment. When base stations want to send commands to thousands of sensor nodes, broadcasting is a much more efficient method than unicasting to each node individually.A wireless sensor network (WSN) can cheaply monitor an environment for diverse industries, such as healthcare, military, or home . A WSN typically consists of several base stations and thousands of sensor nodes, which are resource limited devices with low processing, energy, and storage capabilities.In WSN security,various types of attacks like Denial of service attack,sybil attack,wormhole attack, blackhole attack create problem. Distributing data through wireless communication is also bandwidth limited. A message authentication code (MAC) is an authentication tag derived by applying an authentication scheme and a secret key to a message. MAC is an efficient symmetric cryptographic primitive for two-party authentication; however, MAC is not suitable for broadcast communication without additional modification. Because the sender and its receivers share the same secret key, any one of the receivers can impersonate the sender and forge messages to other receivers. That is, both sender and receivers can sign messages. This problem stems from the symmetric property of MAC. Therefore, to achieve authenticated broadcasts, it is necessary to establish an asymmetric mechanism in which only the sender can sign messages, and the receivers can only verify messages.

II. WSN ARCHITECTURE

WSN architecture[1] is shown in following fig: –

Internet

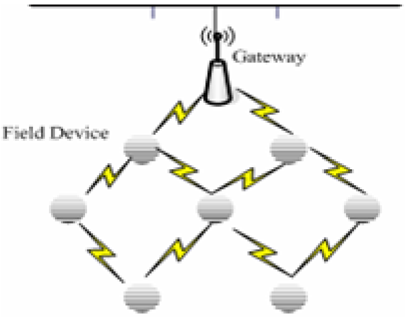

Fig 1 :- An example of WSN

Components:-

• **Sensor motes (Field devices)** – Field devices are mounted in the process, they characterize or control the process or process equipment. A router is a special type of field device that does not have process sensor or control equipment and as such does not interface with the process itself.

• **Gateway or Access points** – A Gateway enables communication between Host application and field devices.

• **Network manager** – A Network Manager is responsible for configuration of the network, scheduling communication between devices, management of the routing tables and monitoring and reporting the health of the network.

• **Security manager** – The Security Manager is responsible for the generation, storage, and management of keys.

III. SECURITY REQUIREMENTS

Sensor networks are used in a number of domains that handle sensitive information. Due to this, there are many considerations that should be investigated and are related with protecting sensitive information traveling between nodes[2].

A. Data Confidentiality

Data confidentiality is the most important issue in network security. Confidentiality requirement is needed to ensure that sensitive information is well protected and not revealed to unauthorized third parties. A sensor network should not leak sensor readings to its neighbors.

B. Authentication

In the case of sensor networks, it is essential for each sensor node and base station to have the ability to verify that the data received was really send by a trusted sender and not by an adversary that tricked legitimate nodes into accepting false data. If such a case happens and false data are supplied into the network, then the behavior of the network could not be predicted and most of times will not outcome as expected.

C. Data Integrity

An adversary may be unable to steal information. However, this doesn’t mean the data is safe. Lack of integrity could result in many problems since the consequences of using inaccurate information could be disastrous. Thus, data integrity ensures that any received data has not been altered in transit.

D. Availability

The wireless sensor network will introduce some extra costs to adjust the traditional encryption algorithms. Availability ensures that services and information can be accessed at the time that they are required. Lack of availability may affect the operation of many critical real time applications. Therefore, it is critical to ensure resilience to attacks targeting the availability of the system and find ways to fill in the gap created by the capturing or disablement of a specific node by assigning its duties to some other nodes in the network.

IV. PROTOCOLS

A Hop-by-Hop Broadcast Source Authentication Protocol[5] for WSN to mitigate DoS Attacks.Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. Broadcast communication is a dominant communication pattern in WSN. As a major security concern, the broadcast source authentication is needed to mitigate impersonation of a broadcast source, modifications of its broadcasted data. Broadcast Source Authentication Protocols (BSAPs); one class of them is time asymmetry-based BSAPs like TESLA protocol. These BSAPs operate delayed key-disclosure to secure broadcast communications, but they suffer from a kind of DoS attack, called resource-draining attack, in which an attacker floods the network with fake messages that all sensors of the network buffer and forward, then later verify, thus causing buffer overflow and batteries depletion. We propose the H2BSAP protocol, to overcome this kind of DoS attacks, by achieving a hop-by-hop authentication of broadcasted messages, thus limiting the damage of an attacker to its one-hop neighbors only, instead of the entire network.In addition, like TESLA[6], H^2BSAP suffers from scalability issue, because it does not efficiently support multiple broadcast sources in the network. An asymmetric mechanism such as public key cryptography is generally required for broadcast authentication. Otherwise, a malicious receiver can easily forge any packet from the sender. uTESLA introduces asymmetry by delaying the disclosure of symmetric keys . A sender broadcasts a message with a Message Authentication Code (MAC) generated with a secret key *K*, which is disclosed after a certain period of time. When a receiver gets this message, if it can ensure that the packet was sent before the key was disclosed, the receiver buffers this packet and authenticates the packet when it later receives the disclosed key. To continuously authenticate broadcast packets, uTESLA divides the time period for broadcast into multiple intervals, assigning different keys to different time intervals. All packets broadcast in a particular time interval are authenticated with the same key assigned to that time interval. Multi-level uTESLA technique to extend the capabilities of uTESLA . The basic idea is to construct a multi-level uTESLA structure, where any higher-level uTESLA instance is only used to authenticate the commitments of its immediate lower-level ones and the lowest level uTESLA instances are actually used to authenticate the data packets. This extension enables the original uTESLA to cover a long time period and support a large number of receivers. Assume a sensor network application requires m uTESLA instances, which may be used by different senders during different periods of time. For convenience, assume m = 2k, where k is an integer. Before deployment, the central server pre-computes m uTESLA instances, each of which is assigned a unique, integer-valued ID between1 and m. Merkle Hash Tree technique is used to authenticate and distribute mTESLA parameters. This method removes the authentication delay as well as the vulnerability to DOS attacks during the distribution of mTESLA parameters, and at the same time allows a large number of senders.

V. COMPARISON BETWEEN MERKLE TREE AND MULTI MTESLA PROTOCOL

Compared with the multi-level mTESLA schemes[7][8] , the most significant gain of the proposed approach is the removal of the authentication delay in distributing the mTESLA parameters. The multi-level mTESLA schemes are subject to DOS attacks against the distribution of mTESLA parameters because of the authentication delay. Specifically, receivers cannot authenticate parameter distribution messages immediately after receiving them, and thus have to buffer such messages. An attacker may send a large amount of messages to consume receivers buffers and thus prevent the receiver from saving the authentic messages.With the proposed approach, senders may still duplicate parameter distribution messages to deal with communication failures. However, unlike multi-level mTESLA schemes, a sender does not have to compete with malicious attackers, since it can immediately authenticate the parameter distribution message instead of keeping it in the buffer for future authentication. In other words, with the proposed approach, it is sufficient for a receiver to receive one copy of each parameter distribution message.In general, our approach allows late binding of mTESLA instances with senders. For example, the central server may reserve some mTESLA instances during deployment time and distribute them to mobile sinks as needed during the operation of the sensor networks. This allows us to add new senders dynamically by simply generating enough number of instances at the central server for later joined senders.

VI. THE EFFICIENT SCHEME

We propose using a cryptographic hash function Hash for example SHA-1[3][10] to construct H as follows
A. split the output of the hash function into k substrings of length log *t* each;[4]
B. interpret each (log *t*)-bit substring as integer written in binary;
C. combine these integers to form the subset of T of size at most k.
We believe that such H satisfies our definition it certainly does if the cryptographic hash function is modeled as a random oracle.
Such construction of H results in the scheme we call HORS (for “Hash to Obtain Random subset”)
This scheme involves three phases and termed as HORS (Hash to Obtain Random Subset).The phases are[12]

1. Key Generation
2. Signing
3. Verifying

Key generation

```
Input : p, d, l
Output: Key Pair
Private Key Kpri  =(k, s1,s2 ,…..,sp)
Public Key Kpub =(k,v1 ,v2 ,…..,vln  d)
1.Randomly generate p l-bit Random numbers as private key.
```

2.Generate public key

Use p balls as pre-image of leaves to build c Merkle trees with height ln p.Take ln d tree root as public key with each public key as sequence period.

3. Distribute Public key.

Signing(Base Station or Sender)

Input: message m, Kpri, one-time session key(k1)

Output: Digital Envelope

1.Encrypt m with k1.

2.Compute Hash(H1) of m.

3.k1 encrypted with Kpri.

Verification(Sensor nodes or receiver)

Input:Digital Envelope

Output:accept or reject

1.Decrypt k1 with its own Kpub

2.Extract original message m with k1

3.Compute Hash(H2) of decrypted message m.

4.Compare H1 wiith H2

If (H1)=(H2)

then output accept;

else output reject:

VII. CONCLUSION

The scheme which we have discussed is also efficient in many ways. As it provides security from adversary that, in any case if it could extract public key that is in transit and get the confidential message out of it. Then the adversary could not encrypt it in the same way as did by the sender. As a result the receiver come to know that there is problem somewhere in transit. Our scheme exhibits many nice properties including individual authentication, robustness to packet loss, and low overhead in computation, communication and storage. This scheme improves upon Hash to Obtain Random Subset (HORS) in terms of reducing the large key storage requirement. This scheme devised a simple and efficient Broadcast Authentication for Wireless Sensor Network.

REFERENCES

[1]. Y. W. Law and P. Havinga. How to secure a wireless sensor network. pages 89–95,Dec. 2005.

[2]. Mayank Saraogi . Security in Wireless Sensor Networks. In ACM SenSys, 2004.

[3]. Huei-Ru Tseng, Rong-Hong Jan and Wuu Yang, "An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks", IEEE Global Communications Conference (GLOBECOM 2007, Washington, DC, USA), pages 986-990, Nov.2007.

[4]. Shang-Ming Chang, Shiuhpyng Shieh, Warren W. Lin, Chih-Ming Hsieh, “An Efficient Broadcast Authentication Scheme in Wireless Sensor Networks”

[5]. D. Liu, P. Ning, S. Zhu, and S. Jajodia, “Practical broadcast authentication in sensor networks,” in Proc.2nd Annual International Conf. Mobile Ubiquitous Syst.: Networking Services (MobiQuitous 2005), July 2005, pp. 118-132.

[6]. Chakib Bekara and Maryline Laurent-Maknavicius and Kheira Bekara InstitutTelecom, Telecom and Management Sud-Paris CNRS Samovar UMR 5157, 9 rue Charles Fourier, 91000 Evry, France,‘H^2BSAP: A Hop-by-Hop Broadcast Source Authentication Protocol for WSN to mitigate DoS attack’.

[7]. Tsern-Huei Lee, “Simple Dynamic User Authentication Protocols for Wireless Sensor Networks”, Second International Conference on Sensor Technologies and Applications (SENSORCOMM’08), pages 657-660, France, 2008.

[8]. D. Liu and P. Ning, “Multi-level mTESLA: Broadcast authentication for distributed sensor networks,” ACM Trans. Embedded Computing Systems (TECS), vol. 3, no. 4, pp. 800-836, 2004.

[9]. I.Akyildiz and I. Kasimoglu, “Wireless sensor and actor networks: research challenges,” Ad Hoc Networks 2(4), pages 351- 367, 2004.

[10]. W. Du, R. Wang, and P. Ning “An efficient scheme for authenticating public keys in sensor networks,” in Proc. 6th ACM International Symposium Mobile Ad Hoc Networking Computing (MobiHoc), 2005, pp. 58-67.

[11]. S. Datema. A Case Study of Wireless Sensor Network Attacks. Master’s thesis, Delft University of Technology,September 2005.

[12]. J. Drissi and Q. Gu, “Localized broadcast authentication in large sensor networks,” in ICNS ’06: Proceedings of the International conference on Networking and Services, 2006, p. 25.