DETECTION AND PREVENTION OF SYBIL ATTACK USING THRESHOLD ELGAMAL KEY MANAGEMENT SCHEME

Jojymon K Thomas[1], Sureshkumar.A[2]

[1]*Department of Computer science, M.E.C, Erode, Anna University (India)*

[2]*Assistant Professor, Department of Computer science, M.E.C, Erode, Anna University (India)*

ABSTRACT

A wireless network is a type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method by using homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure.Analyze several key management schemes that can be used for checking integrity and preventing cloning attacks. After analyzing the problems associated with these schemes It propose a model that allows us to distinguish between legal nodes and cloned nodes in such sensor networks to prevent the Sybil attack as a malicious device criminally taking on multiple identities.To defend against the Sybil attack would like to validate that each node identity is the only identity presented by the corresponding physical node. There are two ways to validate an identity. The first type is direct validation in which a node directly tests whether another node identity is valid. The second type is indirect validation in which nodes that have already been verified are allowed to vouch for or refute other nodes.Here it uses a Elgamal based key management scheme. The ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. It propose a Threshold ElGamal-based key management scheme for protection against Sybil attack.

Keywords: Wireless Sensor Networks, Sybil Attack, Elgamal Key Management Schemes

I. INTRODUCTION

Sensor networks are a promising new technology to enable economically viable solutions to a variety of applications, for example pollution sensing, structural integrity monitoring, and traffic monitoring. A large subset of sensor network applications requires security, especially if the sensor network protects or monitors critical infrastructures .Security in sensor networks is complicated by the broadcast nature of the wireless communication and the lack of tamper-resistant hardware . In addition, sensor nodes have limited storage and computational resources, rendering public key cryptography is impractical.

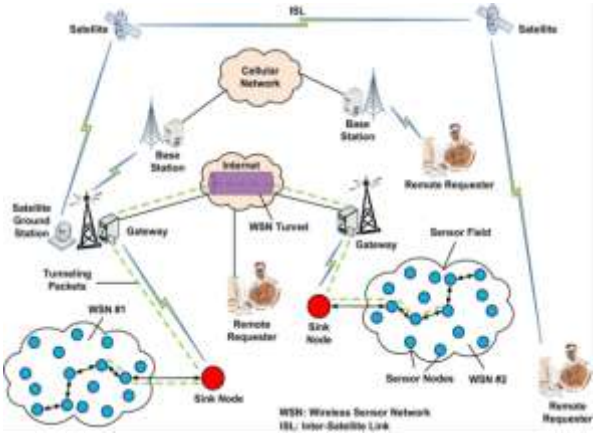

FIG 1 : Wireless Sensor Network Architecture

Wireless Sensor Networks (WSNs) are subject to various kinds of attacks such as replaying of messages, battery exhausting and nodes compromising. While most of these attacks can be dealt with through cryptographic security protocols provided by key management schemes, there are always a few that manage to really cause problems. One such attack that is most common and significant in WSNs is Sybil attack. In Sybil attack the intruder tries to capture and compromise some nodes and inject them into several locations throughout the network in order to conduct other types of attacks. Moreover, if this attack is not detected early, then these replicated injected nodes will consume a large amount of the network resources. Analyze Elgamal key management schemes that can be used for checking integrity and preventing Sybil attacks.

In previous works a distributed hash table (DHT) by which a fully decentralized, key-based caching and checking system is constructed to catch cloned nodes. The protocol's performance on memory consumption and a critical security metric are theoretically deducted through a probability model. DHT-based protocol can detect node clone with high security level and holds strong resistance against adversary's attacks. A Randomly directed exploration, is intended to provide highly efficient communication performance with adequate detection probability for dense sensor networks. In the protocol, initially nodes send claiming messages containing a neighbor-list along with a maximum hop limit to randomly selected neighbours ; then, the subsequent message transmission is regulated by a probabilistic directed technique to approximately maintain a line property through the network as well as to incur sufficient randomness for better performance on communication and resilience against adversary.

II.SYBIL ATTACK

Sybil attack is a harmful attack in sensor networks. In the Sybil attack, a malicious node behaves as if it were a larger number of nodes, for example by impersonating other nodes or simply by claiming false identities. In the worst case, an attacker may generate an arbitrary number of additional node identities, using only one physical device. Wireless Sensor Networks (WSNs) are subject to various kinds of attacks such as replaying of messages, battery exhausting and nodes compromising. While most of these attacks can be dealt with through cryptographic security protocols provided by key management schemes, there are always a few that manage to really cause problems. One such attack that is most common and significant in WSNs is Sybil attack. In Sybil attack the intruder tries to capture and compromise some nodes and inject them into several locations throughout the network in order to conduct other types of attacks. Moreover, if this attack is not detected early, then these replicated injected nodes will consume a large amount of the network resources. Analyze Elgamal key management schemes that can be used for checking integrity and preventing Sybil attacks.

Sensor networks are a talented new technology to enable efficiently feasible solutions to a mixture of applications for example pollution sensing, structural integrity monitoring, and traffic monitoring. Sensor nodes have limited storage and computational resources, rendering public key cryptography impractical. Sybil attack a malicious node behaves like a larger number of nodes for example by impersonating other nodes or simply by claiming false identities. The Sybil attack as a malicious device taking on multiple identities by passing to a malicious device's additional identities as Sybil nodes**.**

2.1 Direct Communication

One way to perform the Sybil attack is for the Sybil nodes to communicate directly with legitimate nodes. When a legitimate node sends a radio message to a Sybil node, one of the malicious devices listens to the message. Likewise, messages sent from Sybil nodes are actually sent from one of the malicious devices

2.2 Indirect Communication

In this version of the attack, no legitimate nodes are able to communicate directly with the Sybil nodes. Instead, one or more of the malicious devices claims to be able to reach the Sybil nodes. Messages sent to a Sybil node are routed through one of these malicious nodes, which pretends to pass on the message to a Sybil node.

2.3 Fabricated Identities

In some cases, the attacker can simply create arbitrary new Sybil identities. If each node is identified by a 32-bit integer, the attacker can simply assign each Sybil node a random 32-bit value.

2.4 Stolen Identities

Given a mechanism to identify legitimate node identities, an attacker cannot fabricate new identities.

2.5 Simultaneous

The attacker may try to have his Sybil identities all participate in the network at once. While a particular hardware entity can only act as one identity at a time, it can cycle through these identities to make it appear that they are all present simultaneously.

2.6 Non-Simultaneous

Alternately, the attacker might present a large number of identities over a period of time, while only acting as a smaller number of identities at any given time. The attacker can do this by having one identity seem to leave the network, and have another identity join in its place. A particular identity might leave and join multiple times, or the attacker might only use each identity once.

III. ElGAMAL PUBLIC KEY CRYTOSYATEM

The ElGamal public key encryption algorithm is based on the discrete log problem and is closely related to Diffe Hellman key exchange. ElGamal PKC that is based on the discrete logarithm problem for , but the construction works quite generally using the DLP . The ElGamal PKC is an example of a public key cryptosystem, so we proceed slowly and provide all of the details. Alice begins by publishing information consisting of a public key and an algorithm. The public key is simply a number, and the algorithm is the method by which Bob encrypts his messages using Alice's public key. Alice does not disclose her private key, which is another number. The private key allows Alice, and only Alice, to decrypt messages that have been encrypted using her public key.

Alice needs a large prime number p for which the discrete logarithm problem in F is difficult, and she needs an element g modulo p of large (prime) order. She may choose p and g herself, or they may have been preselected

by some trusted party such as an industry panel or government agency. Alice chooses a secret number a to act as her private key, and she computes the quantity $\mathbf{A=g^a \pmod p}$

If Bob wants to encrypt a message using Alice's public key A. Bob's message m is an integer between 2 and p. In order to encrypt m, Bob randomly chooses another number k modulo p. Bob uses k to encrypt one, and only one, message, and then he discards it. The number k is called an ephemeral key, since it exists only for the purposes of encrypting a single message. Bob takes his plaintext message m, his chosen random ephemeral key k, and Alice's public key A and uses them to compute the two quantities uses. Bob's cipher text, i.e., his encryption of m, is the pair of numbers which he sends to Alice. Alice decrypt Bob's cipher text Since Alice knows a, she can compute the quantity.

IV. MODULES

4.1 Nodes Unique Identity

All the mobile nodes tend to have a unique id for its identification process, since the mobile nodes communicates with other nodes through its own network id. If any mobile node opted out of the network then the particular node should surrender its network id to the head node.

4.2 Identity Verification

One obvious way to prevent the Sybil attack is to perform identity verification. Verification is likely to be a good initial defense in many scenarios, with the following drawbacks. The list of known identities must be protected from being maliciously modified.

4.3 Location Verification

Another promising approach to defending against the Sybil attack is location verification. In this approach, the network verifies the physical location of each node. While there has been research on automatic location determination, it remains an open research question how to securely verify a node’s exact position.

4.4 Key pool

The key pool scheme randomly assigns k keys to each node from a pool of m keys. During the initialization phase, if any two neighbouring nodes discover that they share q common keys, they can establish a secret link. The problem with this approach is that if an attacker compromises multiple nodes, he can use every combination of the compromised keys to generate new identities. An attacker may attempt to generate new identities to use in the Sybil attack. A usable Sybil identity must be able to pass the validation by other nodes. Validation could be done at different granularities. One extreme is the case of full validation where the sensor network tries to verify as many of a node’s keys as possible, rendering a Sybil attack more difficult.

4.5 Key Management Schemes

Threshold ElGamal system-based key management scheme, cannot get the original plain text with the help of verification process whose number is less than the threshold value. Even if some of the semi-trusted users are physically captured, attackers need to capture threshold of nodes for monitoring. Threshold cryptography achieves the security needs as confidentially and integrity against malicious attackers. It also provides data integrity and availability in a hostile environment and can also employ verification of the correct data sharing. All these can be achieved without revealing the private key.

V. CONCLUTION

In this paper, we define the Sybil attack and we analyzed several key management schemes that can be used for checking integrity and preventing cloning attacks. After analyzing the problems associated with these schemes It propose a model that allows us to distinguish between legal nodes and cloned nodes in such sensor networks to prevent the Sybil attack as a malicious device criminally taking on multiple identities. It includes several steps for detection and prevention of Sybil attack,Nodes unique identity, Identity verification, Location verification, Key pool, Key management schemes. To defend against the Sybil attack would like to validate that each node identity is the only identity presented by the corresponding physical node. There are two ways to validate an identity. The first type is direct validation in which a node directly tests whether another node identity is valid. The second type is indirect validation in which nodes that have already been verified are allowed to vouch for or refute other nodes. Here it uses a Elgamal based key management scheme. The ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. It propose a Threshold ElGamal-based key management scheme for protection against Sybil attack.

REFERENCE

1. A. Shamir, “Identity-based cryptosystems and signature schemes,” in Proc. CRYPTO, 1984, LNCS 196, pp. 47–53.
2. L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” in Proc. 9th ACM Conf. Communication. Security, Washington, DC, 2002, pp. 41–47.
3. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Communication. Mag., vol. 40, no. 8, pp. 102–114, Aug. 2002.
4. Xiaojiang Du, Hsiao-Hwa Chen”Security in wireless sensor networks**”**IEEE Wireless Communications • August 2008 1536-1284/08/ © 2008 IEEE
5. R. Blom. Non-public key distribution. In Advances in Cryptology: Proceedings of Crypto ’82, pages 231–236,1982.
6. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In First IEEE International Workshop on Sensor Network Protocols and Applications, pages 113–127,May 2003.

BIOGRAPHICAL NOTES

Mr.**Jojymon K Thomas** is presently pursuing M.E in communication and networking from **Mahendra engineering college**, Erode, Tamil nadu.

Mr. **Sureshkumar.A** is working as an assistant professor in Computer Science Department,**Mahendra engineering college** , Erode, Tamilnadu.