International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 9 Issue 1 –JULY 2014.

Access Control with Authentication privacy and Intrusion Detection to Secure Data in Wireless Sensor Networks

A.R.Nithya[#1] and C.Renuga[*2]

[#]*PG Scholar, Bharathiyar Arts & Science College for Women*

[*] *Asst., Professor (CSE), Bharathiyar Arts & Science College for Women*

Abstract-The Single sign-on (SSO) is a new authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in a distributed computer network. Recently, Chang and Lee proposed a new SSO scheme and claimed its security by providing well-organized security arguments. In this paper, however, we demonstrative that their scheme is actually insecure as it fails to meet credential privacy and soundness of authentication. Specifically, we present two impersonation attacks. The intermediate nodes along the path to the sink are able to verify the authenticity and integrity of the incoming packets using a predicted value of the key generated by the sender's virtual energy, thus requiring no need for specific rekeying messages. AES is able to efficiently detect and filter false data injected into the network by malicious outsiders.

Keywords: MAN security, GA, cooperative bit-compressed authentication

I. INTRODUCTION

A MAN is usually composed of a large number of sensor nodes which are interconnected through wireless links to perform distributed sensing tasks. Each sensor node is low-cost but equipped with necessary sensing, data processing, and communicating components. Therefore, when a sensor node generates a report after being triggered by a special event.e.g, a while surrounding temperature change, it will send the report to sink through an established routing path. Such nodes are very vulnerable to various security attacks such as selective forwarding, wormholes attacks. In addition, MAN may also suffer from injecting false data attack.

For an injecting false data attack, an adversary first compromises several sensor nodes, accesses all keying materials stored in the compromised nodes and then controls these compromised nodes to inject false information and send those data to the sink to cause upper-level error decision. Therefore, it is crucial to filter the false data as accurately as possible in MAN which results in energy deprivation. To tackle this challenging issue, some false data filtering mechanisms have been developed.

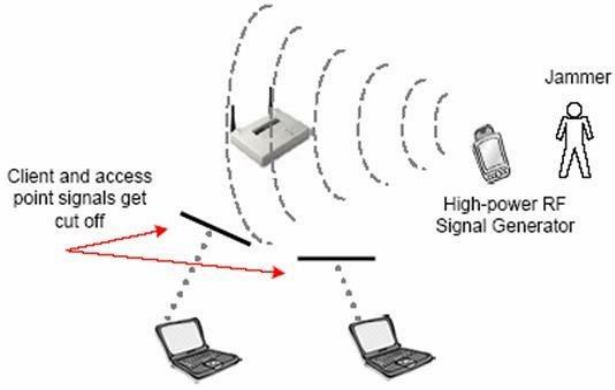

Fig: Effect of SSO in wireless network

II. BACKGROUND WORK

Prior Filtering mechanisms use the symmetric key technique when the node is compromised. Those can abuse its keys to generate false reports and the reliability of the filtering mechanisms is degraded which makes hard to identify the node. Ye et al. propose a statistical en-routing filtering Mechanism called SEF. It requires each sensing report be validated by multiple keyed message authenticated (MACs). Each generated by a node detects the same event. As the report being forwarded, each node along the way verifies the correctness of the MACs at earliest point. If the injected false data escapes the en-routing filtering and is delivered to the sink to verify the correctness of each MAC carried in each report and reject false ones. In SEF, to verify the MACs, each node gets a random subset of the keys of size k from the global key pool of size N and uses them to producing the MACs. To save the bandwidth, SEF adopts the bloom filter to reduce the MAC size. SEF does not consider the possibility of compromise nodes which is crucial to the false data filtering.

Zhu et al. present an interleaved hop-by-hop authentication (IHA) scheme for filtering of injected false data. In IHA, each node is associated with two other nodes along the path, one is the lower association node and the other is the upper

association node. An en-routing node will forward receive report if it is successfully verified by its lower association node. To reduce the size of the report, the scheme compresses individual MACs by XOR-ing them to one. However, the security of the scheme is mainly subject upon the creation of associations in the association discovery phase. Once the creation fails, the security cannot be guaranteed. Location-Based Resilient Secrecy (LBRS), adopts location key binding mechanism to reduce the damage caused by node compromise, and further mitigates the false data generation in MAN. It propose location-aware end-to-end data security design (LEDS) to provide end-to-end security guarantee including efficient en-routing false data filtering capability and high-level assurance on data availability. Because LEDS is a symmetric key based solution, to achieve en-routing filtering, it requires location-aware key management, where each node should share at least one authentication key with one node in its upstream/downstream report.

Zhang et al. provide a public key based solution to the same problem. Especially, they propose the notion of location-based keys by binding private keys of individual nodes to both their IDs and geographic locations and a suite of location-based compromise-tolerant security mechanisms. To achieve en-routing filtering, additional 20 bytes authentication overheads are required. Bit-compressed authentication technology achieves bandwidth-efficiency. Canetti et al. use one-bit authentication to achieve multicast security. The basic idea in multicast is very similar to the BECAN scheme, where a source knows a set of keys, each recipient knows a subset of them. When the source sends a message M, it authenticates M with each of the keys using MAC. Each recipient verifies MACs which were created using the keys in its subset. If any of these MACs is incorrect, the message M will be rejected. To achieve the bandwidth efficiency, each MAC is compressed as single bit. The security of the scheme is based on the assumption that the source is not compromised. However, once the source is compromised the scheme obviously does not work. Therefore, it cannot be applied to filter false data injected by compromised nodes.

Sensed Results Reporting Protocol

When a sensor node generates a report after being triggered by a special event or response to a query from the sink, it will send the report to the sink via established routing.

En-Routing Filtering

When each sensor node along the routing receives the message (m, T, MAC) from its upstream node, it checks the integrity of the message m and the timestamp T. If the timestamp T is out of date, the message (m, T, MAC) will be discarded. Otherwise, Ri invokes the Algorithm called cooperative neighbor router (CNR) MAC verification. If the returned value is “accept” Ri will forward the message (m, T, MAC) to its downstream node, Otherwise discard.

Sink Verification

If the sink receives the report (m, T, MAC), it checks the integrity of the message m and the timestamp T. If the timestamp is out of date, the report (m, T, MAC) will be immediately discarded. Otherwise, the sink looks up all private keys and invokes Sink verification Algorithm. If the returned value of Algorithm is “accept,” the sink accepts. Otherwise rejects the report.

Disadvantages of existing system

1. Reliability:

If at least one report reaches the sink, the true event will successfully report else BECAN scheme cannot filter injected false data.

2. Scalability:

In the BECAN scheme, the additional authentication bits are in linear with the length of the path L. If L is too long, the authentication bits become large.

3. BECAN scheme is efficient for injecting false data by single attackers but not in case of group attackers.

Future extensions

1. To prevent gang injecting false data attack from mobile compromised sensor nodes.

2. To resolve the scalability issue, develop a large-scale sensor network into a heterogeneous sensor network, where each partition consists of High-end sensor and Low-end sensors.

III. PROPOSED SYSTEM

An identity (ID)-based signature scheme allows any pair of users to communicate securely and to verify each other’s signatures without exchanging public key certificates. The proposed new ID based signature scheme that allows batch verification of multiple signatures.

Using the new scheme, the signature size is reduced into almost half and efficiently verify multiple signatures. The verification cost of k signatures by a single signer is one signature verification plus k elliptic curve addition and k hashing. When a new signature by a different signer is added, additional verification cost is almost a half of that of ordinary verification of a single signature with minimal security loss.

If there is an attacker who can forge a set of signatures to pass batch verification, then the computational Diffie-Hellman problem (CDHP) is used to solve such problem. Batch verification was devised to improve the efficiency of verification process for multiple signatures.

Proposed technique description: An ID-based Signature

This scheme consists of four algorithms: Setup, Extract, Signing and Verification.

Setup

Given a GDH group G and its generator P, pick a random s $\in$ Z/`Z and set Ppub = sP. Choose two hash functions H1 : {0,

1}∗ × G → (Z/`Z)∗ and H2 :{0, 1}∗ → G∗. The system parameter is (P, Ppub,H1,H2). The master key is s.

Extract

Given an identity ID, the algorithm computes QID = H2(ID) and DID =sH2(ID) and outputs DID as a private key of the identity ID corresponding to QID = H2(ID).

Signing

Given a secret key DID and a message m, pick a random number r ∈ Z/`Z and output a signature σ = (U, V) where U = rP, h = H1(m,U), and V = rQID+hDID.

Verification

Given a signature σ = (U, V) of a message m for an identity ID, compute h = H1(m,U). The signature is accepted if and only if (P,QID,U + hPpub, V) is a valid Diffie-Hellman tuple AES Aggregate Verification

A forger is given a target public key for which a forged signature should be made. While each secret key of users is chosen independently in the traditional public key system, all secret keys of users are mutually related in ID-based system. In fact, they are produced from one secret key of the whole system. Hence in ID-based setting it is reasonable not to give specific ID but a system parameter to a forger.

K-aggregate forger of a chosen ID:

A forger succeeds if he can produce a set of k signatures which pass the aggregate verification. This type of forger is known as k-aggregate forger of a chosen ID.

K-aggregate forger of a given ID:

A forger produces a set of k signatures one of which has the signer with the given ID, then this type of forger is called a k-aggregate forger of a given ID.

IV. CONCLUSION

SSOM signature scheme is more secure and deploys efficent batch verification. Aggregated Signature is a generalized version of Batch Signature where many signatures for different messages signed by different signers are aggregated into one signature and verified by one equation.

V. REFERENCE

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “MAN: A Survey,” Computer Networks, vol. 38, no. 4, pp. 393-422, Mar. 2002.

[2] C. Vu, R. Beyah, and Y. Li, “A Composite Event Detection in Wireless Sensor Networks,” Proc. IEEE Int’l Performance, Computing, and Comm. Conf. (IPCCC ’07), Apr. 2007.

[3] S. Uluagac, C. Lee, R. Beyah, and J. Copeland, “Designing Secure Protocols for Wireless Sensor Networks,” Wireless Algorithms, Systems, and Applications, vol. 5258, pp. 503-514, Springer, 2008.

[4] Crossbow Technology, http://www.xbow.com, 2008. [5] G.J. Pottie and W.J. Kaiser, “Wireless Integrated Network Sensors,” Comm. ACM, vol. 43, no. 5, pp. 51-58, 2000.

[5] R. Roman, C. Alcaraz, and J. Lopez, “A Survey of Cryptographic Primitives and Implementations for Hardware-Constrained Sensor Network Nodes,” Mobile Network and Applications, vol. 12, no. 4, pp. 231-244, Aug. 2007.

[6] H. Hou, C. Corbett, Y. Li, and R. Beyah, “Dynamic Energy-Based Encoding and Filtering in Sensor Networks,” Proc. IEEE Military Comm. Conf. (MILCOM ’07), Oct. 2007.

[7] L. Eschenauer and V.D. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” Proc. Ninth ACM Conf.