An Overview on Message Authentication Scheme in Wireless Sensor Network

Shital Pawde

M.E. Student, Dr. Bhausaheb Nandurkar College of Engineering and Technology, Yavatmal, Maharashtra.

Abstract: Wireless Sensor Network consists of a large number of sensor nodes. Each sensor node knows its location in the sensor domain and is capable of communicating with its neighbouring nodes directly using geographic routing.Message authentication plays a prominent role in thwarting unauthorized and corrupted messages from being forwarded in networks to save the sensor energy. Many authentication schemes have been developed to provide message authenticity and integrity verification for wireless sensor networks. Many of these schemes are based on either symmetric-key cryptosystems or public-key cryptosystems. Many of them, however, have the restrictions of high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks.Wireless Sensor Networks (WSN) are being very popular day by day, however one of the main concern in WSN is its limited resources. One have to look to the resources to generate Message Authentication Code (MAC) keeping in mind the feasibility of method used for the sensor network at hand. This paper investigates different cryptographic approaches such as symmetric key cryptography and asymmetric key cryptography.

Keyword- Wireless sensor networks (WSNs), symmetric-key cryptosystem, public-key cryptosystem, source privacy, Hop-by-hop authentication.

INTRODUCTION

The primary purpose of deploying a wireless sensor network (WSN) is to monitor the physical world and provide observations for various applications. As WSNs are usually deployed in an environment that is vulnerable to many security attacks, it is critical to control the access to the sensor nodes (e.g., reading sensor data), especially when there are many users in the system.Message authentication performs a very important role in thwarting unauthorized and corrupted messages from being delivered in networks to save the valuable sensor energy. Therefore, many authentication schemes have been proposed in literature to offer message authenticity and integrity verification for wireless sensor networks (WSNs). These approaches can largely be separated into two categories: public-key based approaches and symmetric-key based approaches.

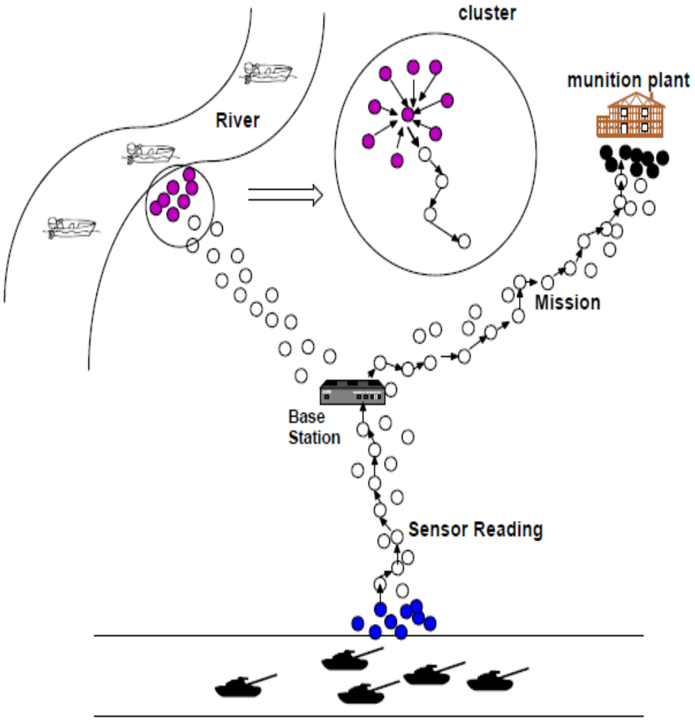

Figure 1 Wireless Sensor Network

The symmetric-key based approach necessitates composite key management, lacks of scalability, and is not flexible to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. The shared key is handled by the sender to produce a message authentication code (MAC) for each transmitted message. However, for this process the authenticity and integrity of the message can only be confirmed by the node with the shared secret key, which is usually shared by a group of sensor nodes. An intruder can compromise the key by incarcerating a single sensor node. In addition, this method is not useful in multicast networks. For the public-key based method, each message is transmitted along with the digital signature of the message produced using the sender's private key. Every intermediate forwarder and the final receiver can authenticate the message using the sender's public key. One of the restrictions of the public key based method is the high computational overhead.

THREAT MODEL AND ASSUMPTIONS

The WSNs are assumed to consist of a large number of sensor nodes. We assume that each sensor node knows its relative location in the sensor domain and is capable of communicating with its neighbouring nodes directly using geographic routing. The whole network is fully connected through multi-hop communications. We assume there is a security server (SS) that is responsible for generation, storage and distribution of the security parameters among the network. This server will never be compromised. However, after deployment, the sensor nodes may be captured and compromised by attackers. Once compromised, all information stored in the sensor nodes can be accessed by the attackers. The compromised nodes can be reprogrammed and fully controlled by the attackers. However, the compromised nodes will not be able to create new public keys that can be accepted by the SS and other nodes.

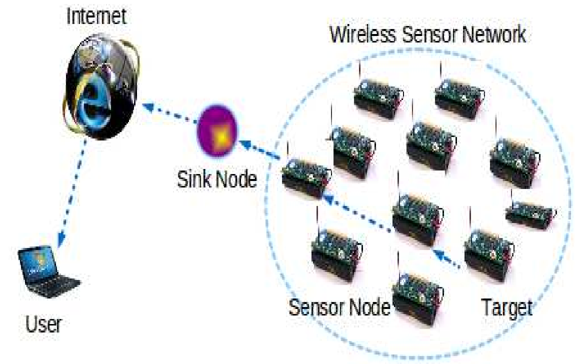

Figure 2: Typical multi-hop wireless sensor network architecture

Based on the above assumptions, this paper considers two types of attacks launched by the adversaries:

- Passive attacks. Through passive attacks, the adversaries could eavesdrop on messages transmitted in the network and perform traffic analysis.
- Active attacks. Active attacks can only be launched from the compromised sensor nodes. Once the sensor nodes are compromised, the adversaries will obtain all the information stored in the compromised nodes, including the security parameters of the compromised nodes. The adversaries can modify the contents of the messages, and inject their own messages.

DESIGN GOALS

Message authentication scheme should aims at achieving the following goals:

- **Message authentication**. The message receiver should be able to verify whether a received message is sent by the node that is claimed or by a node in a particular group. In other words, the adversaries cannot pretend to be an innocent node and inject fake messages into the network without being detected.
- **Message integrity**. The message receiver should be able to verify whether the message has been modified en-route by the adversaries. In other words, the adversaries cannot modify the message content without being detected.
- **Hop-by-hop message authentication**. Every forwarder on the routing path should be able to

verify the authenticity and integrity of the messages upon reception.

- **Identity and location privacy**. The adversaries cannot determine the message sender's ID and location by analyzing the message contents or the local traffic.
- **Node compromise resilience**. The scheme should be resilient to node compromise attacks. No matter how many nodes are compromised, the remaining nodes can still be secure.
- **Efficiency**. The scheme should be efficient in terms of both computational and communication overhead

INSIDE VIEW ON WIRELESS SENSOR NETWORKS

Wireless sensor networks simplify the compilation and scrutiny of information from multiple locations. The term wireless sensor network (WSN) illustrates an association among miniaturized embedded communication devices that supervise and evaluate their surrounding environment. The network is composed of many minute nodes sometimes referred to as motes. A node is made up of the sensor(s), the microcontroller, the radio communication component, and a power source. Wireless sensor nodes range in size from a few millimetres to the size of a handheld computer.

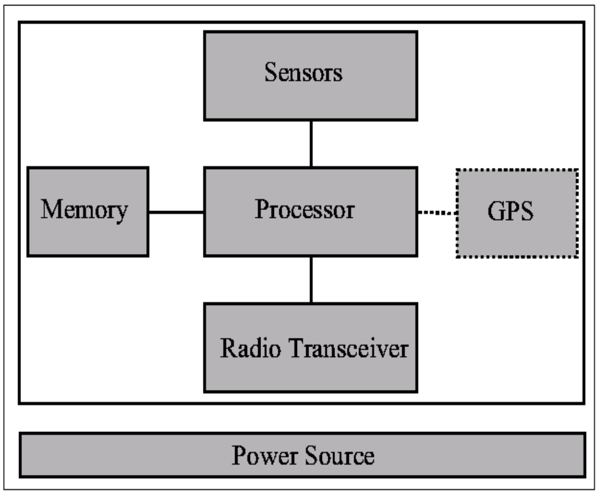

Figure 3: Basic Components of a WSN Node

RELATED WORK

- Multicast stream authentication and signing is an important and challenging problem. Applications include the continuous authentication of radio and TV Internet broadcasts, and authenticated data distribution by satellite. The main challenges are fourfold. First, authenticity must be guaranteed even when only the sender of the data is trusted as the most prominent security risk from a user point of view is data authenticity. Second, the scheme needs to scale to potentially millions of receivers. Third, streamed media distribution can have high packet loss. Finally, the system needs to be efficient to support fast packet rates. The paper [1], propose two efficient schemes, TESLA and EMSS, for secure lossy multicast streams. TESLA, short for Timed Efficient Stream Loss-tolerant Authentication, offers sender authentication, strong loss robustness, high scalability, and minimal overhead, at the cost of loose initial time synchronization and slightly delayed authentication. EMSS, short for Efficient Multi-chained Stream Signature, provides non repudiation of origin, high loss resistance, and low overhead, at the cost of slightly delayed verification.

TESLA has the following properties:

1) **Low computation overhead**. The authentication involves typically only one MAC function and one hash function computation per packet, for both sender and receiver.
2) **Low per-packet communication overhead**. Overhead can be as low as 10 bytes per packet.
3) **Arbitrary packet loss tolerated**. Every packet which is received in time can be authenticated.
4) **Unidirectional data flow**. Data only flows from the sender to the receiver. No acknowledgments or other messages are necessary after connection setup. This implies that the sender's stream authentication overhead is independent on the number of receivers, so our scheme is very scalable.
5) **No sender-side buffering**. Every packet is sent as soon as it is ready.
6) **High guarantee of authenticity**. The system provides strong authenticity. By strong authenticity we mean that the receiver has a

high assurance of authenticity, as long as our timing and cryptographic assumptions are enforced.

7) **Freshness of data**. Every receiver knows an upper bound on the propagation time of the packet.

The main features of EMSS are:

- It amortizes the cost of a signature operation over multiple packets, typically about one signature operation per 100 to 1000 packets
- It tolerates high packet loss.
- It has low communication overhead, between 20 to 50 bytes per packet, depending on the requirements.

- A statistical En-route filtering mechanism (SEF) proposed [2] to serve applications that work in an adverse or even hostile environment, such as battlefield surveillance and forest fire monitoring. A sensor network must not only report each relevant event promptly, but also reject false reports injected by attackers. In addition to causing false alarms that can waste real-world response effort, false reports can drain out the finite amount of energy resource in a battery-powered network. In a large-scale sensor network, detecting and purging bogus reports injected by compromised nodes is a great research challenge. Once a node is compromised, all the security information stored in that node becomes accessible to the attacker.

  SEF exploits the sheer scale and dense deployment of large sensor networks. To prevent any single compromised node from breaking down the entire system, SEF carefully limits the amount of security information assigned to any single node, and relies on the collective decisions of multiple sensors for false report detection. A report with an inadequate number of MACs will not be delivered. As a sensing report is forwarded towards the sink over multiple hops, each forwarding node verifies the correctness of the MACs carried in the report with certain probability. Once an incorrect MAC is detected, the report is dropped. The probability of detecting incorrect MACs increases with the number of hops the report travels.

  In any case the sink will further verify the correctness of each MAC carried in each report and reject false ones.

  The contribution of this paper is two-fold. First, we propose a key assignment method designed for en-route detection of false reports in the presence of compromised nodes. Second, we devise mechanisms for collective data report generation, en-route report filtering, and sink verification. Results show that SEF is able to detect and drop 80-90% injected reports by a compromised node within 10 forwarding hops, thus reducing energy consumption by 50% or more in many cases.

  SEF achieves its goal by carefully limiting the amount of security information assigned to each individual node. The more security information each forwarding node possesses, the more effective the en-route filtering can be, but also the more secret the attacker can obtain from a compromised node. So we need evaluation of the tradeoffs between these two conflict goals.

- Sensor networks are often deployed in unattended environments, thus leaving these networks vulnerable to false data injection attacks in which an adversary injects false data into the network with the goal of deceiving the base station or depleting the resources of the relaying nodes. Standard authentication mechanisms cannot prevent this attack if the adversary has compromised one or a small number of sensor nodes. Paper [3], present an interleaved

  Hop-by-hop authentication scheme that guarantees that the base station will detect any injected false data packets when no more than a certain number t nodes are compromised.

  Further, scheme provides an upper bound B for the number of hops that a false data packet could be forwarded before it is detected and dropped, given that there are up to t colluding compromised nodes. Shown from performance analysis that scheme is efficient with respect to the security it provides, and it also allows tradeoffs between security and performance.

  This paper presents a scheme for addressing the form of attack, which we call a false data injection attack. The scheme enables the base station to verify the authenticity of a report that it has received as long as the number of compromised sensor nodes does not exceed a certain threshold. Further, the scheme attempts to filter out false data packets injected into the network by compromised nodes before they reach the base station, thus saving the energy for relaying them.

- Yanchao Zhang, Wei Liu propose LBK based on pairing and LTE [4]. Their main contributions are summarized as follows.

  First, propose the novel notion of location-based keys (LBKs) based on a new cryptographic concept called pairing. In the scheme, each node holds a private key bound to both its ID and geographic location rather than merely ID as in conventional schemes.

  Second, design a novel node-to-node neighbourhood authentication protocol based on LBKs. It helps achieve the desirable goal of localizing the impact of compromise nodes (if any) to their vicinity, which is a nice property absent in most previous proposals.

  Third, present efficient approaches to establish pair wise hared keys between any two nodes that are either immediate neighbours or multi hop away. Such keys are fundamental in providing security support for WSNs. In contrast to previous proposals, this approaches feature low communication and computation overhead, low memory requirements, and good network scalability. More important, these approaches show perfect resistance to node compromise in those pair wise shared keys between non compromised nodes always remain secure, no matter how many nodes are compromised.

  Fourth, we demonstrate how LBKs can act as efficient countermeasures against some notorious attacks against WSNs. These include the Sybil attack, the identity replication attack, wormhole and sinkhole attacks, and so on.

  Finally, we develop a location-based threshold-endorsement scheme (LTE) to thwart the aforementioned bogus data injection attack. Detailed performance evaluation shows that LTE can achieve remarkable energy savings by detecting and dropping bogus traffic at their early transmission stages. Moreover, LTE has a much higher level of compromise tolerance than previous work.

- The recent progress of elliptic curve cryptography (ECC) implementation on sensors motivates to design a public-key scheme and compare its performance with the symmetric-key counterparts. The paper [5] proposes an ECC-based access control for sensor networks, which consists of pair wise key establishment, local access control, and remote access control and have performed a comparison test by implementing both symmetric-key and public-key primitives on popular sensor motes. The experiment results suggest public key based protocol is more advantageous than the symmetric key in terms of the memory usage, message complexity, and security resilience.

- Most of the message authentication schemes have the following limitations: high computation or communication overhead, no resilience to a large number of node compromises, delayed authentication, lack of scalability, etc. To address these issues, Subramanian and Wang propose [6] a new message authentication approach to address the aforementioned limitations. The approach has following features: lightweight in terms of computation, communication and storage overhead; resilience to a large number of sensor node compromises; immediate authentication (therefore supporting both synchronous and asynchronous communication); scalability; and non-repudiation. These features are attained by applying a number of novel techniques: Firstly, they adopt polynomials for message authentication, which provides higher adaptability than existing authentication techniques based on multiple MACs , and at the same time, keeps the advantage of immediate authentication held by those techniques. Secondly, messages are authenticated and verified via evaluating polynomials, which incurs lower overhead than existing asymmetric cryptography-based authentication techniques such as digital signature. Thirdly, independent and random factors are employed to perturb polynomial shares (of a system-wide secret polynomial) that preloaded to individual nodes, which significantly increases the complexity for the intruder to break the secret polynomial, and therefore renders the proposed approach to be resilient to node compromises. This method achieves simultaneously the features of compromise-resiliency, flexible-time authentication, efficiency and non-repudiation without employing public key cryptography.

- A wireless sensor networks is composing of a great lot sensors. Each sensor is usually limited power, computation, storage, sensing and communication capabilities. The major challenge of employing a public key security scheme directly in wireless sensor networks is the limited resources budgets of sensors participating in the network. Among several public key schemes, Elliptic Curve Cryptography (ECC) based algorithms have proven acceptable performance for low powered sensor nodes. Considering both the software and hardware configurations, elliptical curve based public key cryptography (PKC) has shown relatively better result.

  The paper [7], propose a security architecture based-on public key cryptography. The scheme can ensure a good level of security and is very much suitable for the resources constrained trend of wireless sensor network, which is built on the basis of an identity based cryptosystem in the flat network topological structure of wireless sensor networks.

  In future we can study the use of PKC to the hierarchical network topological structure and the mixed network topological structure of WSN.

- Ren, Ren and Zhang investigated techniques to achieve the efficient and lightweight data integrity check for in-networking storage WSNs [8]. They summarize a technique called Two Granularity Linear Code (TGLC), which can check data integrity efficiently and also propose a scheme based on TGLC that has two advantages: checking the data integrity in a distributed manner, and having low communication overhead.

  In In-networking storage Wireless Sensor Networks, sensed data are stored locally for a long term and retrieved on-demand instead of real-time. To maximize data survival, the sensed data are normally distributivelly stored at multiple nearby nodes. It arises a problem that how to check and grantee data integrity of distributed data storage in the context of resource constraints. The present technique called Two Granularity Linear Code (TGLC) consists of Intracodes and Inter-codes is an efficient and lightweight data integrity check scheme based on TGLC is proposed. Data integrity can be checked by anyone who holds short Intercodes, and the checking credentials are short Intra-codes that are dynamically generated. The scheme is efficient and lightweight with respect to low storage and communication overhead, and yet checking validity is maintained. Conclusion is justified by extensive analysis.

- A distributed access control module in wireless sensor networks (WSNs) allows the network to authorize and grant user access privileges for in-network data access. Prior research mainly focuses on designing such access control modules for WSNs, but little attention has been paid to protect user's identity privacy when a user is verified by the network for data accesses.

  Often, a user does not want the WSN to associate his identity to the data he requests. The paper [9], present the design, implementation, and evaluation of a novel approach, Priccess, to ensure distributed privacy-preserving access control. In Priccess, users who have similar access privileges are organized into the same group by the network owner. A network user signs a query command on behalf of his group and then sends the signed query to the sensor nodes of his interest. The signature can be verified by its recipient as coming from someone authorized without exposing the actual signer.

- Jian Li, Jian Ren propose an unconditionally secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified ElGamal signature

(MES) scheme on elliptic curve cryptography (ECC). The scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power. While achieving compromise resiliency, flexible-time authentication and source identity protection, the scheme does not have the threshold problem. Both theoretical analysis and simulation results demonstrate that proposed scheme is more efficient than the polynomial-based algorithms in terms of computational and communication overhead under comparable security levels while providing message source privacy.

CONCLUSION

This paper discusses an overview on message authentication in wireless sensor networks. Message authentication performs a key role in thwarting unauthorized and corrupted messages from being forwarded in networks. It investigates that symmetric-key based approach requires complex key management, lacks of scalability, and is not resilient to large numbers of node compromise attacks. The recent progress on elliptic curve cryptography (ECC) shows that the public key schemes can be more advantageous in terms of computational complexity, memory usage, and security resilience, since public-key based approaches have a simple and clean key management. The SAMA scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power, achieving compromise resiliency, flexible-time authentication and source identity protection, the scheme does not have the threshold problem.

REFERENCES

1) Perrig, R. Canetti, J. Tygar, and D. Song, "**Efficient Authentication and Signing of Multicast Streams over Lossy Channels**," Proc. IEEE Symp. Security and Privacy, May 2000.
2) F. Ye, H. Lou, S. Lu, and L. Zhang, "**Statistical En-Route Filtering of Injected False Data in Sensor Networks**", Proc. IEEE INFOCOM, Mar. 2004
3) 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.
4) Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang, "**Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks",** IEEE Journal on selected areas in communications, vol. 24, no. 2, february 2006.
5) H. Wang, S. Sheng, C. Tan, and Q. Li, "**Comparing Symmetric-Key and Public-Key Based Security Schemes in Sensor Networks: A Case Study of User Access Control**," Proc. IEEE 28th Int'l Conf. Distributed Computing Systems (ICDCS), pp. 11-18, 2008.
6) W. Zhang, N. Subramanian, and G. Wang, "**Lightweight and Compromise-Resilient Message Authentication in Sensor Networks"**, Proc. IEEE INFOCOM, Apr. 2008.
7) Jianbo Yao, Zunyi Guizhou, "**A Security Architecture for Wireless Sensor Networks Based-on Public Key Cryptography**", IEEE 2009.
8) Wei Ren, Yi Ren, Hui Zhang,**"Efficient and Lightweight Data Integrity Check in In-Networking Storage Wireless Sensor Networks",** 2009 IEEE International Symposium on Parallel and Distributed Processing with Applications.
9) Daojing He, Jiajun Bu, Sencun Zhu, Sammy Chan, and Chun Chen, "**Distributed Access Control with Privacy Support in Wireless Sensor Networks**" IEEE 2011.
10) Jian Li, Yun Li, Jian Ren and Jie Wu, "**Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks**", IEEE transactions on parallel and distributed systems, vol. 25, no. 5, may 2014.