SURVEY ON PROVENANCE BASED MECHANISM FOR DETECTING FORGERY AND PACKET DROP IN WIRELESS SENSOR NETWORK

Ms. Shweta Hiremath[1], Ms. Karthikayini[2]
[1]PG Student, [2]Assistant Professor, Department of Computer Science and Engineering
New Horizon College of Engineering, Bangalore, Karnataka, India

Abstract: As the wireless sensor network continue to grow the need for effective security mechanism has increased. The highly sensitive nature of the information collected from the various nodes in wireless sensor network makes security a critical concern. When the data is transferred from one node to another there is possibility the malicious adversary may introduce the additional nodes in the network or compromise the existing nodes. Many traditional methodologies like cryptography and digital signature were used to provide security. Identification of suitable cryptography for wireless sensor networks is an important challenge due to limitation of energy, computation capability and storage resources of the sensor nodes. Symmetric based cryptographic schemes do not scale well when the number of sensor nodes increases. Hence public key based schemes are widely used. We present here two public – key based algorithms, RSA and Elliptic Curve Cryptography (ECC) and found out that ECC have a significant advantage over RSA as it reduces the computation time and also the amount of data transmitted and stored.
Keywords: data, nodes, security

I. INTRODUCTION

Wireless sensor network is used in numerous applications such as military monitoring, health care as well as civilian applications. Wireless sensor network consists of sensor nodes which consist of in built battery and processor for some data processing. It also consists of small radio bandwidth range. It becomes necessary to provide security to the data in the network from the various attacks. Wireless sensor nodes transmit data from one node to another it becomes target for malicious attack. In these kind of situation attackers may create traffic collision, or may damage nodes physically, misdirect or drop message in routes. Security in WSN is a greater challenge in WSN due to the processing limitations of sensor nodes and nature of wireless links. Extensive use of WSNs is giving rise to different types of threats. Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy, nonrepudiation, and anti-playback. The more the dependency on the information provided by the networks has been increased, the more the risk of secure transmission of information over the networks has increased. To defend against the threats proper security schemes are required. Traditionally security is implemented through hardware or software and is generally achieved through cryptographic methods. Limited area, nature of links, limited processing, power and memory of WSNs leads to strict constraints on the selection of cryptographic techniques. The goal of security services in WSNs is to protect the information and resources from attacks and misbehavior. The security requirements in WSN include:

1. Confidentiality: Confidentiality is hiding the information from unauthorized access. In many applications, nodes communicate highly sensitive data. A sensor network should not leak sensor reading to neighbouring networks. Simple method to keep sensitive data secret is to encrypt the data with a secret key that only the intended receivers possess, hence achieving confidentiality.
2. Authentication: Authentication ensures the reliability of the message by identifying its origin. In a WSN, the issue of authentication should address the following requirements (i) communicating node is the one that it claims to be(ii)the receiver should verify that the received packets have undeniably come from the actual sensor node.
3. Integrity: Integrity is preventing the information from unauthorized modification. Data authentication can provide data integrity also.
4. Availability: Availability ensures that services and information can be accessed at the time they are required. In sensor networks there are many risks that could result in loss of availability such as sensor node capturing and denial of service attacks.

A wireless sensor network (WSN) consists of a collection of nodes that have the facility to sense, process data and communicate with each other via a wireless connection. Grouping sensor nodes into clusters has been widely adopted by the research community to satisfy the above scalability objective and generally achieve high energy efficiency and prolong network lifetime in large-scale WSN environments. In network structure each cluster has a leader, which is also called the cluster head (CH) and usually performs the special tasks like fusion and aggregation, and several common sensor nodes (SN) as members. The cluster formation process eventually leads to a two-level hierarchy where the CH nodes form the higher level and the cluster-member nodes form the lower level. The sensor nodes periodically transmit their data to the corresponding CH nodes. Each node is allotted a distance value and the node with highest distance value is marked as cluster head. The data transmission between the clusters is known as inter-cluster communication and the data transmission with in the cluster

is known as intra-cluster communication. The node which sends the data encrypts it and at the receiving end the data is decrypted which also contains the path followed, source node and the data. For encryption and decryption Elliptical curve cryptography algorithm is used.

II. LITERATURE SURVEY

Koustuv Dasgupta, Konstantinos Kalpakis, Parag Namjoshi:" An Efficient Clustering–based Heuristic for Data Gathering and Aggregation in Sensor Networks"

Advantage:

- It has advantage; the clustering step arranges spatially co-related sensors into a cluster.
- It limits the number of sensors in a MASTER-tree which restricts the exponentially large number of association rules into a more manageable number.

Disadvantage:

- DEMS makes use of virtual static sensors that tackles the problems of location-aware clustering of real mobile sensors.

Ian Foster, Jens Vöckler, Michael Wilde, Yong Zhao:" Chimera: A Virtual Data System for Representing, Querying, and Automating Data Derivation"

Advantage:

- It couples the Chimera system with distributed "Data Grid" services to enable on-demand execution of computation schedules constructed from database queries

Disadvantage:

- It has two challenge problems, the reconstruction of simulated collision event data from a high-energy physics experiment, and the search of digital sky survey data for galactic clusters, with promising results.

Christian Esteve Rothenberg, Carlos A. B. Macapuna, Maur´ıcio F. Magalhaesa, F´abio L. Verdib, Alexander: "In-packet Bloom filters: Design and networking applications"

Advantage:

- It has ability to provide Bloom filter, algorithms, distributed systems.

It has some feature packet forwarding, inter-networking.

Disadvantage:

- The practical limitation appears to be solely how much space to store the candidate element representations the application designer is willing to pay.

Tilman Wolf: "Data Path Credentials for High-Performance Capabilities-Based Networks"

Advantage:

- Instead of permitting the transmission of packets from any source to any destination, routers deny forwarding by default.

Disadvantage:

- A major challenge for a high-performance implementation of such a network is an efficient design of the credentials that are carried in the packet and the verification procedure on the router.

Adam Kirsch, Michael Mitzenmacher: "Distance-Sensitive Bloom Filters"

Advantage:

- The potential benefits of this type of data structure are its speed and space

Disadvantage:

- It experiments suggest that even with this limitation distance-sensitive Bloom filters work sufficiently well to be useful in practice.

Ragib Hasan, Radu Sion, Marianne Winslett : "The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance"

Advantage:

- It can perform quick verification. The auditor may choose to disregard the linear checksum.

Disadvantage:

- Major drawbacks include the fact that the logic and higher level data management semantics are not naturally propagated to the kernel, thus limiting the types of provenance related inferences that can be made.

III. METHODOLOY

Elliptical curve cryptography (ECC) Algorithm:

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. Because ECC helps to establish equivalent security with lower computing power and battery resource usage.

Advantages of ECC over RSA:

1. Shorter keys are as strong as long key for RSA.
2. Low on CPU consumption.
3. Low on memory usage.
4. Size of encrypted data is smaller

Selection of cluster head:

Each node is allotted a distance value the node which has the highest distance value is set as the cluster head.

Detection of Attacker:

Based on the time constraint the malicious node is identified taking into consideration the duration of time required for data to reach source node to destination node and the data is not decrypted when malicious node is encountered.

IV. CONCLUSION

This paper proposed Elliptical curve cryptography algorithm that helps to enhance the security of the wireless sensor

network by encrypting the data at source node and decrypting at destination node and identifying the malicious node present in the path of data transmission and eliminating the misuse of data by the attackers. Only one transmission of data at instant of time is done to avoid the collision and loss of data. The ECC algorithm used in this paper it reduces the computation time and also the amount of data transmitted and stored.

REFERENCES

[1] H. Lim, Y. Moon, and E. Bertino, "Provenance-Based Trustworthiness Assessment in Sensor Networks," Proc. Seventh Int'l Workshop Data Management for Sensor Networks, pp. 2-7, 2010.

[2] I. Foster, J. Vockler, M. Wilde, and Y. Zhao, "Chimera: A Virtual Data System for Representing, Querying, and Automating Data Derivation," Proc. Conf. Scientific and Statistical Database Management, pp. 37-46, 2002.

[3] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance-Aware Storage systems," Proc. USENIX Ann. Technical Conf., pp. 4-4, 2006.

[4] Y. Simmhan, B. Plale, and D. Gannon, "A Survey of Data Provenance in E-Science," ACMSIGMODRecord, vol. 34, pp. 31-36, 2005.

[5] R. Hasan, R. Sion, and M. Winslett, "The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance, "Proc. Seventh Conf. File and Storage Technologies (FAST), pp. 1-14, 2009.

[6] S. Madden, J. Franklin, J. Hellerstein, and W. Hong, "TAG: A Tiny Aggregation Service for Ad-Hoc Sensor Networks," ACM SIGOPS Operating Systems Rev., vol. 36, no. SI, pp. 131-146, Dec. 2002.

[7] K. Dasgupta, K. Kalpakis, and P. Namjoshi, "An Efficient Clustering Based Heuristic for Data Gathering and Aggregation in Sensor Networks," Proc. Wireless Comm. and Networking Conf., pp. 1948-1953, 2003.

[8] S. Sultana, E. Bertino, and M. Shehab, "A Provenance Based Mechanism to Identify Malicious Packet Dropping Adversaries in Sensor Networks," Proc. Int'l Conf. Distributed Computing Systems (ICDCS) Workshops, pp. 332-338, 2011.

[9] L. Fan, P. Cao, J. Almeida, and A.Z. Broder, "Summary Cache: A Scalable Wide-Area Web Cache Sharing Protocol," IEEE/ACM Trans. Networking, vol. 8, no. 3, pp. 281-293, June 2000.

[10] A. Kirsch andM. Mitzenmacher, "Distance-Sensitive BloomFilters," Proc.Workshop Algorithm Eng. and Experiments, pp. 41-50, 2006.

[11] C. Rothenberg, C.Macapuna,M.Magalhaes, F. Verdi, and A. Wiesmaier, "In-Packet Bloom Filters: Design and Networking Applications," Computer Networks, vol. 55, no. 6, pp. 1364-1378, 2011.

[12] M. Garofalakis, J. Hellerstein, and P. Maniatis, "Proof Sketches: Verifiable In-Netwok Aggregation," Proc. IEEE 23rd Int'l Conf. Data Eng. (ICDE), pp. 84-89, 2007.

[13] T. Wolf, "Data Path Credentials for High-Performance Capabilities-Based Networks," Proc. ACM/IEEE Symp. Architectures for Networking and Comm. Systems, pp. 129-130, 2008.

[14] H. Chan, A. Perrig, and D. Song, "Secure Hierarchical In-Network Aggregation in Sensor Networks," Proc. Conf. Computer and Comm. Security (CCS), pp. 278-287, 2006.

[15] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure Data Aggregation in Wireless Sensor Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 3, pp. 1040-1052, June 2012.

