Shodhshauryam, International Scientific Refereed Research Journal
© 2018 SISRRJ | Volume 1 | Issue 4 | ISSN : 2581- 6306

Secure Group Communication Using Elliptic Curve Cryptography in WSN

Binu Ruby Sunny[1], P. Parthasarathi[2], Prof. S. Shankar[3]

[1]PG Scholar, Department of CSE, Akshaya College of Engineering and Technology, Malumichampatti, Tamil Nadu, India

[2]Assistant Professor, Department of CSE, Akshaya College of Engineering and Technology, Malumichampatti, Tamil Nadu, India

[3]Professor and Head, Department of CSE, Hindustan College of Engineering and Technology, Malumichampatti, Tamil Nadu, India

ABSTRACT

Sensor devices are vulnerable of malicious attacks. These kinds of attacks extract the most confidential information which is exchanged between the devices. In order to protect these kinds of data, it must be secured from view. The mechanism of protecting the data is done by cryptographic procedures. Many type of attack is executed by taking the node identity as input parameter. By taking the advantage of hiding the identity information from packet is lead to protect and prevent the malicious attacks during communication. To establish this type of communication strategy, anonymous communication is used which takes the secured parameter as input instead of node identity. Key updation is the second most important factor which makes the communication is secured. The key must be updated during two situations for all users in the secured group. The two situations are, user joins in group, user leaves from group.

Keywords : Sensors, Key Updation, Secure Communication.

I. INTRODUCTION

Sensor networks consist of large numbers of wireless sensor nodes which have only limited memory as well as limited computational and communication capabilities. After deployment, they operate unattended and without physical protection. They need to communicate with each other to accumulate data and (possibly) relay the data to a base station. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

1.1 Wireless Sensor Network

Wireless sensor networks are being deployed in a wide variety of scenarios including hostile environments where adversaries may be present. WSN refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind, and so on. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust,

although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

1.2 Secure Group Communication Systems

A Group Communication System (GCS) consists of the following five common operations: initiate, join, leave, partition, and merge. The group is first established by initial members. Then one or several potential members join the group while some members leave the group. This is so-called dynamic membership. A large number of membership changes, referred to as a bulk membership change, may require a specialized protocol design without demeaning group performance. In some scenarios a group can be divided into smaller subgroups or fused into a bigger group. This is also considered as a bulk membership change, but the transitions among groups likely incur overheads. This dynamic membership aspect requires the Group Communication Systems to rekey the session keys in order to preserve the key secrecy.

All nodes learn each other's virtual addresses and cryptographic keys. The final address tree is verifiable after network convergence, and all forwarding decisions can be independently verified. Furthermore, assuming each legitimate network node has a unique certificate of membership (assigned before network deployment), nodes who attempt to join multiple groups, produce clones of themselves in multiple locations, or otherwise cheat during discovery can be identified and evicted as topology discovery. Discovery begins with a time limited period during which every node must announce its presence by broadcasting a certificate of identity, including its public key (from now on referred to as node ID), signed by a trusted offline authority.

II. LITERATURE SURVEY

WSN is emerging technology for numerous area in recent years. Its application developed for areas including medical, industrial, agricultural, home appliance and military applications. These are similar to wireless ad hoc networks in the sense that they rely on wireless connectivity and spontaneous formation of networks so that sensor data can be transported wirelessly.

2.1 Title "Scalable Hierarchical Access Control in Secure Group Communications," (Author: Y. Sun and K.J.R. Liu)

In hierarchical management scenarios, many group communications require security infrastructure that ensures multiple levels of access privileges for group members. The multi-group key management scheme that achieves such a hierarchical access controls by employing an integrated key graph and managing group keys for all users with different access privileges. Compared with applying existing key management schemes directly to the hierarchical access control problem, here the scheme significantly reduces the overhead associated with key management and achieves better scalability when the number of access levels increases. In addition, here the key graph is suitable for both centralized and contributory environments.

2.2 Title "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage," (Author: B.J. Cui, Z.L. Liu, and L.Y. Wang)

Over incidental information spills in the cloud there might be enormous wide security worries with various clients through open distributed storage due

to the capacity of specifically scrambled information sharing. In any case, for both encryption and pursuit, to clients need of disseminating safely and to safely store the got keys likewise suggests those clients will have to perform and seek over the common information and submit to the cloud all together a just as vast number of watchword trapdoors. The idea of instantiating through the plan of a solid KASE and proposing the idea of key-total searchable encryption (KASE), it addresses this down to earth issue. The future work is that, under multi-proprietors setting, how to diminish the quantity of trapdoors.

2.3 Title "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage," (Author: C.K. Chu, S.S.M. Chow, W.G. T zeng , J. Zhou, and R.H. Deng.)

Cloud computing provides the flexible architecture to share the applications as well as the other network resources. Cloud storage enables networked online storage. Key management and key sharing plays the main role in the data sharing concept of cloud computing. Here, Cipher text policy attribute-based encryption (CP-ABE) is introduced with Key aggregate cryptosystem as a promising cryptographic solution to this issue. It enables data owners to define their own access policies over user attributes and enforce the policies on the data to be distributed and Attribute policies , Cipher text policies are being aggregated. This effectively eliminates the need to rely on the data storage server for preventing unauthorized data access and integrity.

2.4 Title "Verifiable Searchable Encryption with Aggregate Keys for Data Sharing System," (Author: Z.L. Liu, T. Li, P. Li, and et al.,)

Data sharing is an important aspect in cloud storage. Here we show how to securely, efficiently, and flexibly share data with others in cloud storage. It describes new public-key cryptosystems which produce constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts are possible. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated. Here it provides formal security analysis of our schemes in the standard model. The other application of our schemes is described. In particular, our schemes give the first public-key patient-controlled encryption for flexible hierarchy, which was yet to be known.

III. SYSTEM MODEL

The fundamental security service in SGC is the provision of a shared key, the group key. The shared group key is used to encrypt a group message, authenticate members and messages, sign the message, and authorize access to traffic and group resources.

3.1 Proposed System

In cryptographic functions, a trapdoor is a common concept that defines a one-way function between two sets. A global trapdoor is an information collection mechanism in which intermediate nodes may add information elements, such as node IDs, into the trapdoor. Only certain nodes, such as the source and destination nodes can unlock and retrieve the elements using pre-established secret keys. The usage of trapdoor requires an anonymous end-to-end key agreement between the source and destination. The route request packets are authenticated by a secured identity, to defend the potential active attacks without unveiling the node identities. The key-encrypted information with a route secret verification message is designed to prevent intermediate nodes from inferring a real destination.

IV. SYSTEM IMPLEMENTATION

In sensor network the flow of data is very important aspect because each data packet contains the event which may be very important for some application.

So the data transmission must be secured. But sensor node has limited energy and limited memory capacity so maintaining security is difficult for them. To make the data transmission secure some basic aspects of security has to be maintained during transmission. The authentication and confidentiality maintained is discussed during data transmission because without this two parameter data transmission cannot be reliable. The system has following implementation modules

1. Setting up the security model
2. Key generation and key sharing
3. Node Anonymity
4. Routing model
5. Hash code generation
6. Encryption decryption with data access
7. Key validation

Reliable data transfer with no data loss

Normally data transfer has to be reliable and make sure that no data is lost during the transmission. So there are two basic methods by which data is transfer from one node to another node reliably.

1. **Acknowledgement based method:** A node waits for an acknowledgement from receiver after sending the packet to receiver. It waits for a time period (ta). If no acknowledgment receives within this time period then sender again re-transmits the data packet and this process continues until sender gets the acknowledgement for that data packet from receiver.
2. **Non acknowledgement based method**: In Non-ack based method sender send the first data packet to the receiver. After that it send the next data packet without waiting for acknowledgement of the previous sent data packet because here no acknowledgement is used. Now after receiving the next data packet the receiver can realize that previous data packet has not been received by the receiver; so it send a RMP request for that missing data packet. After receiving this RMP sender only send that requested data packet. So this is the main working mechanism for non-ack based method.

V. RESULT AND DISCUSSION

The simulation is conducted using the ns-2 simulator, which is a discrete event simulator. This simulator is used to test the performance of the existing protocols as well as newly derived protocols. Here, the simulation is conducted to test the quality of the proposed protocol, which is designed to improve the scalability network protocols. The proposed system is compared with existing protocol which creates the secured group communication in the sensor network. The performance evaluation is conducted to validate the execution of the proposed technique in terms of packet related metrics such as PDR, delay, throughput, Overhead, Normalized Overhead.

RESULT

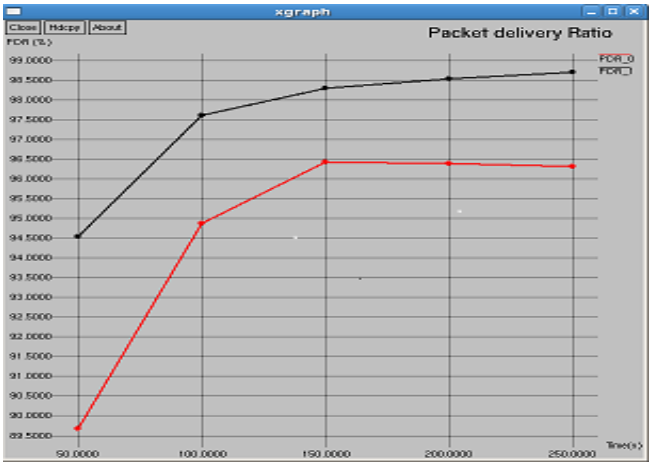

Fig 1 Packet delivery ratio

VI. CONCLUSION& FUTURE WORK

CONCLUSION

Due to limited resources and size constrain of a node, WSN still lacks a comprehensive security mechanism for its operations. A good key pre-distribution scheme should be resilient to node compromise. Key updating is the most important factor which makes the communication is secured. The performance evaluation showed that the proposed system

achieved the better performance compare to the existing cryptographic method in terms of packet delivery ratio, Transmission Delay, Throughput, Control Overhead, Normalized Overhead, Good put and Jitter

FUTURE WORKS

It can further enhance by designing the methodology with the energy constraints during the data transmission. The system should maintain the forward secrecy and backward secrecy in batch communication along with the Dual Authentication. In cryptographic functions, a trapdoor is a common concept that defines a one-way function between two sets. A global trapdoor is an information collection mechanism in which intermediate nodes may add information elements, such as node IDs, into the trapdoor. Only certain nodes, such as the source and destination nodes can unlock and retrieve the elements using pre-established secret keys. The key-encrypted information with a route secret verification message has to be designed to prevent intermediate nodes from inferring a real destination.

VII. REFERENCES

[1]. Anoop , M. (2007). Elliptic curve cryptography , an implementation guide.X. ANSI (1998). 63: Public key cryptography for the financial services industry, key agreement and key transport using elliptic curve cryptography. American National Standards Institute.

[2]. Rafaeli, S., & Hutchison, D. (2003). A survey of key management for secure group communication. ACM Computing Surveys.

[3]. J. Shen, H. W. Tan, J. Wang, J. W. Wang, and S. Y. Lee, “A Novel Routing Protocol Providing Good Transmission Reliability in Underwater Sensor Networks,”

[4]. Z.H. Xia, X.H. Wang, X.M. Sun, and Q. Wang, “A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data,”

[5]. Z.L. Liu, T. Li, P. Li, and et al., “Verifiable Searchable Encryption with Aggregate Keys for Data Sharing System,” Future Generation Computer Systems, accepted 12 February 2017

[6]. C.K. Chu, S.S.M. Chow, W.G. Tzeng, J. Zhou, and R.H. Deng, “Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 468-477, Feb. 2014

[7]. B.J. Cui, Z.L. Liu, and L.Y. Wang, “Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage,” IEEE Transactions on Computers, vol. 65, no. 8, pp. 2374-2385, Aug. 2016

[8]. Y. Sun and K.J.R. Liu, “Scalable Hierarchical Access Control in Secure Group Communications,” Proc. IEEE INFOCOM ’04, Hong Kong, China, 2004, pp. 1296-1306.