© 2019 IJSRSET | Volume 6 | Issue 3 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology
DOI : 10.32628/IJSRSET196324

Hybrid Key Generation for Securing the Sensor Cloud

Binu Ruby Sunny[1], P. Parthasarathi[2], Prof. S. Shankar[3], Dr. N. Suguna[4]

[1]PG Scholar, Akshaya College of Engineering and Technology

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

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

[4]Professor, Akshaya College of Engineering and Technology, Tamil Nadu, India

ABSTRACT

Sensor devices are susceptible to a variety of attacks including the black hole, wormhole and denial of service attacks. These kinds of attacks extract the most confidential information which is exchanged between the devices. First, to make sensor networks economically viable, sensor devices are limited in their energy, computation, and communication capabilities. Second, unlike traditional networks, sensor nodes are often deployed in accessible areas, presenting the added risk of physical attack. And third, sensor networks interact closely with their physical environments and with people, posing new security problems. When setting up a sensor network, one of the first requirements is to establish cryptographic keys for later use. Cryptography entails a performance cost for extra computation that often increases packet size. Cryptographic hardware support increases efficiency but also increases the financial cost of implementing a network. Many types of attack are executed by taking the node identity as input parameter. By taking the advantage of hiding the identity information from the packet is lead to protect and prevent the malicious attacks during communication. Identity-based encryption is a public-key encryption in which the public-key of a user can be set as an identity-string of the user. There is a private key generator (PKG) in IBE which holds a master-secret key, and issues a secret key to each user with respect to the user identity. During data access, for both uploading and downloading process shared key is used to protect the data. The performance evaluation shows that the proposed Hybrid Key Generation System (HKGS) for securing the WSN achieves the best performance compare to the existing Secured Group Communication Using ECC (SGCUE) in terms of the packet delivery ratio, Transmission Delay, Throughput, Control Overhead, Normalized Overhead, Goodput and Jitter.

Keywords : Sensors, Communication, Security, Wireless Network, PKG, SGCUE

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. The sensor nodes are usually distributed randomly in a certain area for data acquisition and environment monitoring. 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.

Wireless networks are vulnerable to sybil attacks due to the broadcast nature of the wireless medium. Location distinction can tell whether or not all

identities are originated from the same location, and thus detect such attacks. In wireless networks, location distinction aims to detect location changes or facilitate authentication of wireless users. The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in networks.

II. LITERATURE SURVEY

2.1 J. Byun, and S. Park, "Development of a self-adapting intelligent system for building energy saving and context-aware smart services," IEEE Trans. Consumer Electron., vol. 57, no. 1, pp. 90-98, Feb. 2011.

In case there is no trustworthy home in the community, the source home may apply classic layered encryption technique to establish an anonymous route to the destination. The idea is to assign a session key to every hop along the route and encrypt each data packet in layers, using theses keys in accordance with the order of the hops in the route. Intermediate nodes are informed by the source about the session keys of their incidental hops through a route establishment phase. They peel off one encryption layer from a received data packet and retransmit the packet to all the nodes in its communication range including the next hop. The destination removes the last encryption layer and obtains the original data packet. In this way, home privacy can be preserved since no intermediate node is aware of the source, the destination, or even other intermediate nodes.

2.2 W. Noh, and T. Kim, "Flexible communication-bus architecture for distributed multimedia service in cloud computing platform," IEEE Trans. Consumer Electron., vol. 59, no. 3, pp. 530-537, Aug. 2013.

A home gateway is considered unreliable if it either fails to forward messages or transmits incorrect messages. Having unreliable gateways in the community network may increase communication delay and cause bandwidth waste, data loss, and communication failure. The reasons for a home gateway to appear unreliable are multifold: error-prone wireless media, software faults and hardware defects. Network attacks also contribute to home gateway unreliability. An adversary may occupy the wireless channel by overwhelming frequencies of illegitimate traffic so that legitimate traffic is jammed. It may compromise several home gateways, access all keying materials stored on them, and then control them to disseminate bogus data to the community and/or the service center, degrading the fidelity of the propagated information and leading to erratic upper-level decisions. Reliable communication is expected in the presence of unreliable home gateways.

2.3 Z. Fu, J. Shu, X. Sun, and N. Linge, "Smart cloud search services: Verifiable keyword-based semantic search over encrypted cloud data," IEEE Trans. Consumer Electron., vol. 60, no. 4, pp. 762-770, Nov. 2014.

Cloud-Based Services Regarding Household Living: To achieve high-level home automation, third-party servers and configured smart home systems are recommended to address data privacy and authentication concerns in interhome, multiple-device smart environments. Smart home systems have been extended to intelligent building systems, with both indoor and outdoor scenarios being involved. User terminals and servers must be hierarchically connected to develop data communication channels. Software updating must consider regional software distribution. Using cloud resources must entail security functions for accessing personal and group data. To manage faults in the smart home systems, the cloud servers must cooperate with the core resource that manages the local servers to diagnose the faults through comparisons of events at different time points.

2.4 P. A. Cabarcos, F. A. Mendoza, R. S. Guerrero, A. M. Lopez, and D. Diaz-Sanchez, "SuSSo: Seamless and ubiquitous single sign-on for cloud service continuity across devices," IEEE Trans. Consumer Electron., vol. 58, no. 4, pp. 1425-1433, Nov. 2012.

The home network is formed by a number of home automation systems (e.g., healthcare systems and security systems) for continuous real-time monitoring of residents, the home environment, and the nearby community environment (e.g., the street segments beside a house). These systems report their surveillance results to a home gateway inside the home in a single-hop or multi-hop way. The connection may be realized by power line communication technologies such as Home Plug, wireless communication technologies like Bluetooth, phone line communication technologies such as HomePNA (www.homepna.org), or other technologies such as Ethernet that require dedicated wiring. The gateway is the home's communication interface with the outside world. It is able to intelligently process and manage gathered surveillance data, provide efficient paths for forwarding them to other homes or the remote community center in the community domain via wireless networks, and/or enable immediate contact with the call center in the service domain for response.

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. A Group Key Management scheme used in any secure group communication system should satisfy the following requirements:

- Imitation of the group key should be infeasible or computationally difficult.
- Key generation is secure.
- The group key is securely distributed and only the legitimate users can receive a valid group key.
- A rekeying of the key is secure.
- Revocation of the group key upon every membership change should be immediate.

III. 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. RESULT AND CONCLUSION

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 Hybrid Key Generation for Securing the Sensor Cloud is compared with the Existing Secure Group Communication using ECC in WSN. 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. The table shows that the parameters used to perform the network simulation.

V. REFERENCES

[1]. J. Byun, and S. Park, "Development of a self-adapting intelligent system for building energy saving and context-aware smart services," IEEE Trans. Consumer Electron., vol. 57, no. 1, pp. 90-98, Feb. 2011.

[2]. W. Noh, and T. Kim, "Flexible communication-bus architecture for distributed multimedia service in cloud computing platform," IEEE Trans. Consumer Electron., vol. 59, no. 3, pp. 530-537, Aug. 2013.

[3]. Z. Fu, J. Shu, X. Sun, and N. Linge, "Smart cloud search services: Verifiable keyword-based semantic search over encrypted cloud data," IEEE Trans. Consumer Electron., vol. 60, no. 4, pp. 762-770, Nov. 2014.

[4]. P. A. Cabarcos, F. A. Mendoza, R. S. Guerrero, A. M. Lopez, and D. Diaz-Sanchez, "SuSSo: Seamless and ubiquitous single sign-on for cloud service continuity across devices," IEEE Trans. Consumer Electron., vol. 58, no. 4, pp. 1425-1433, Nov. 2012.

Cite this article as :

Binu Ruby Sunny, P. Parthasarathi, Prof. S. Shankar, Dr. N. Suguna, "Hybrid Key Generation for Securing the Sensor Cloud", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 6 Issue 3, pp. 89-92, May-June 2019.

Journal URL : http://ijsrset.com/IJSRSET196324