International Journal of Computer & Mathematical Sciences
IJCMS
ISSN 2347 – 8527
Volume 7, Issue 5
May 2018

Secured Message Exchange in Mission Critical Infrastructure using Conditional Privacy Preserving Authentication

Dr. Rajasekar Rangasamy
Professor/CSE, St.Peters Engineering College, Hyderabad.
Dr. H. Shaheen
Associate Professor / CSE, St.Peters Engineering College, Hyderabad.

ABSTRACT

Wireless Sensor Networks (WSNs) received enormous attention in recent years due to its phenomenal ability of implementation in various fields. WSNs consist of a large number of small sensor nodes. These nodes are very cheap in terms of cost. In military operations, there is always a threat of being attacked by enemies. So, the use of these cheap sensor nodes will help to reduce the loss. In this project, the security of data transmission in WSNs for military applications is analyzed. It discusses the available scenarios of using sensor nodes in the military uses. The aim is to present a better deployment of sensor nodes for military purposes with the help of cryptographic techniques.

This project will try to identify different areas in which we can reduce the damage in case of militant's attack or enemy's outbreak using an intelligent deployment of nodes. It is proposed to use the WSNs in battlefield surveillance to closely monitor the critical areas and borders to obtain information about enemy activity in that area. Hence, militant's will gather information quickly which will result in quick response. Border monitoring is an essential component of military surveillance to prevent enemy's intrusion. Here the proposed work provides security using several techniques to encrypt and decrypt the data in WSNs. Elliptic Curve cryptography involves Attribute based encryption which is more complicate to hack. As well as skipjack is used to create digital signature to avoid unauthorized users.

INTRODUCTION

The rise of Wireless Sensor Networks(WSNs) has brought revolution in the field of technology. These networks comprise of a large number of densely deployed sensor nodes which works through collaboration. In WSNs, each sensor node has limited resources such as, low energy, less bandwidth, limited memory and small computational power These nodes are very inexpensive in terms of cost, so resource limitation is not a big problem. If a node runs out of energy, so instead of replacing the battery, user can replace the entire node with a new node. There are different types of sensors available like temperature sensor, humidity sensor, multimedia sensor and others. Due to these variant sensors, WSNs got applications in different fields such as environment monitoring, agriculture monitoring, industrial monitoring, health monitoring, home applications and military operations.

Sensor Networks were initially designed for military operations and surveillance. WSNs have been emerged as an excellent tool for military applications involving intrusion detection, various parameters monitoring, information gathering and, smart logistics support in an unknown deployed area. These networks can provide different services to military and air force like information collection, battlefield surveillance and attack detection. Because of their capabilities of real time transmission, WSNs play an important role in military operations. These networks offer several advantages over traditional sensor devices such as fault tolerance, robustness and low budget deployment. In case of enemy attack, some nodes will be damaged but node damage in WSNs does not disturb the complete network.

It is proposed to use the WSNs in battlefield surveillance to closely monitor the critical areas and

borders to obtain information about enemy activity in that area. Hence, user will gather information quickly which will result in quick response. Another way of using sensor nodes for battlefield surveillance is as the operations advance and new operational arrangements are ready, new sensor systems could be conveyed for front observation. Both the approaches are good. Everyone have its advantages. Border monitoring is an essential component of military surveillance to prevent enemy's intrusion. Using Elliptic Curve Integration Scheme user id is registered and digital signature is created using skipjack algorithm. Key is issued for Communication.

Private Key, Secret key and Timestamp is generated from the server. TA maintains user registration. Set source id and destination id, key is exchanged for communication. Upload sender message to send to destination. Before sending the message, encrypt the message with MAC code. Conditional Privacy Preserving Authentication scheme is used to update the hash chain value. It updates user action, whether user is in revoked or in non-revoked status. After verifying the sender the message is decrypted. Thus communication between sender and receiver will be more secure.

There exist various studies about implementing WSNs in military applications. Authors discussed these applications in different parts of military operations from different perspectives. In, different areas are pointed where WSNs can be deployed in order to obtain better results and desired outputs. These areas include intrusion detection, enemy tracking and target classification, battlefield surveillance, battlefield damage assessment, target system and detection of Nuclear Biological Chemical (NBC) attacks. WSNs use one to one communication to transfer data securely. The WSNs in military applications focus on maximizing the security of the data transmission.

The challenging problem is how to effectively transfer data securely between two communicating parties in military operations and surveillance. Obviously users can transfer their data securely, but once the key is lost then the data will be hacked by unauthorized user. Here the proposed work considered these problems and provides security using several techniques to encrypt and decrypt the data in WSNs. This mission critical infrastructure is more efficient and provides secure data transmission between sender and receiver.

Wireless sensor networks(WSNs) are widely used to collect data. However, WSNs are usually deployed in unattended or hostile environment in which an adversary might attempt to introduce fraudulent data into the WSNs and cause error decision at upper level. Therefore, data authentication is desired in WSNs. In addition, in some applications(e.g. military applications), privacy is also an inevitable problem, which threatens the security of networks.

However, existing data authentication schemes only provide authentication, but pay no attention to privacy. In Proposed project a data authentication scheme providing privacy preservation based on encryption scheme, pseudonym technology and message authentication code. Theoretical analysis shows that this scheme not only provides data authentication and privacy preservation, but also has a good performance in terms of communication and computation overhead.

The proposed scheme also has advantages in security compared to prior solutions and analyzes the security of the scheme using BAN logic. The base station could authenticate messages from sensor nodes to avoid receiving false reports. Compared to the existing schemes, this scheme not only achieves data authentication, but also protects the end-to-end data privacy and nodes location privacy. In addition, Theoretical analysis shows that this scheme also has advantages in terms of security, communication and computation overhead compared to prior solutions.

Mobile nodes in military environments like in battlefield or a hostile region area unit possible to suffer from intermittent network property and frequent partitions. Disruption tolerant network(DTN) technologies have become production solutions that enable wireless devices carried by soldiers to speak with one another and access the direction or command reliably by exploiting secondary storage nodes A number of the most difficult problems during this situation area unit the social control of authorization policies and therefore the policies update for secure knowledge retrieval.

Cipher text-policy attribute-based encryption(CP-ABE) is a promising scientific discipline resolution

to the access management problems. However, the matter of applying CP-ABE in decentralized DTNs introduces many security and privacy challenges with relation to the attribute revocation, key escrow, and coordination of attributes issued from completely different authorities. Tend to propose a secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes severally.

Demonstrate the way to apply the projected mechanism to securely and efficiently manage the confidential knowledge distributed in the disruption-tolerant military network. Disruption Tolerant Network(DTN) technologies are a unit designed to specific applications comparable to military applications where ever soldiers use wireless devices to speak with each other and access the direction dependably by mistreatment storage devices nodes. CP-ABE is a ascendable cryptographic solution to access and provide security for data retrieval. Tend to plan an efficient and secure management of information retrieval technique by using CP-ABE for DTNs where ever multiple key authorities manage their attributes severally.

Here these tend to resolved key escrow agreement such that the secrecy of the storage node is not visible even under the some extreme situations such as key authorities might be combined together.

The rapidly developing ad hoc network technology has a wide range of applications, such as vehicular ad hoc network(VANET), wireless sensor network (WSN), emergency and military communications. Due to the characteristics such as openness and dynamic topology, ad hoc networks suffer from various attacks in data plane. Even worse, some attacks can subvert or bypass the frequently used identity based security mechanisms. In order to secure the data plane of ad hoc networks, a novel trust management system is proposed.

In the system, fuzzy logic is employed to formulate imprecise empirical knowledge, which is used to evaluate path trust value. Together with fuzzy logic, graph theory is adopted to build a novel trust model for calculating node trust value. To defend against increasing attacks to trust management systems, such as slandering and harboring, a filtering algorithm is used.

An efficient trustworthiness decay method is also designed to resolve the conflict about decaying historical trust value in trust based routing decision. Additionally, it present a feasible trust factor collection approach to assure the trust management system is compatible with other security primitives, such as encryption and encapsulation. Finally, it implement the proposed trust management system by integrating it into the optimized link state routing (OLSR) protocol. Simulation results show that the proposed trust management system works well in detecting and resisting data plane attacks.

Fuzzy logic and graph theory are employed to construct the trust model, which is able to formulate the imprecision of empirical knowledge and is suitable for distributed networks. In order to obtain correct and objective node trust value, a filtering algorithm is presented. Moreover, a simple but efficient trustworthiness decay method is designed to facilitate the enforcement of the proposed trust mechanisms in routing decision. FGT-OLSR framework demonstrates that the implementation of trust management system is feasible and easy. Simulation results also show that trust management system is effective and efficiency in protecting data plane of ad hoc networks.

PROPOSED SYSTEM

Proposed work is simultaneously providing a security and an efficient data transfer between users. The construction proposed work is deliberately designed to meet these two above goals. To achieve efficient data transfer, improve the existing by using new techniques. Elliptic Curve Integrated Encryption Scheme (IES) is a hybrid encryption scheme which provides semantic security against an adversary who is allowed to use chosen-plaintext and chosen-cipher text attacks. Elliptic Curve cryptography involves Attribute based encryption which is more complicate to hack. The security of the scheme is based on the Diffie–Hellman problem. Two incarnations of the IES are standardized: Discrete Logarithm Integrated Encryption Scheme (DLIES) and Elliptic Curve Integrated Encryption Scheme (ECIES), which is also known as the Elliptic Curve Augmented Encryption Scheme or simply the Elliptic Curve Encryption Scheme.

These two incarnations are identical up to the change of an underlying group and so to be concrete we concentrate on the latter. ECIES combines a Key Encapsulation Mechanism (KEM) with a Data Encapsulation Mechanism (DEM). The system independently derives a bulk encryption key and a MAC key from a common secret. Data is first encrypted under a symmetric cipher, and then the cipher text is Mac's under an authentication scheme. Finally, the common secret is encrypted under the public part of a public/private key pair. The output of the encryption function is the tuple {K, C, T}, where K is the encrypted common secret, C is the cipher text, and T is the authentication tag. There is some hand waiving around the "common secret" since it's actually the result of applying a Key Agreement function, and it uses the static public key and an ephemeral key pair. ECIES and Skipjack technique is used to register in server.

Skip jack is used to create digital signature. Skipjack uses an 80-bit key to encrypt or decrypt 64-bit data blocks. Skipjack is an unbalanced Feistel network with 32 rounds. It was designed to used in secured phones. In the revocation processes, the values of the hash chains are continuously used, and hence, the Trusted Authority can consume all the hash chain values. As an end result, there should be a mechanism to replace the current hash chain with a new one. The symmetric cryptographic algorithm uses a key to encrypt the encrypted message using two escrowed keys. The encrypted key and an identifier of the chip that sent it are encrypted again with a "family key." The two escrowed keys are combined to decrypt the key that decrypts the message.

CONCLUSION

WSNs play an important role in military operations. With the help of these networks, not only the critical areas can be monitored but also due to its flexible nature, it can be expanded to the nearby areas according to the requirements with the passage of time. Moreover due to its fault tolerance characteristic, if any node got damaged, the rest of the network will continue sensing. Rest of the network will not be affected due to the damage of a single or a group of sensors. The use of Wireless Sensor Networks (WSNs) will reduce the casualty rate. Normally these networks are deployed in risky and critical areas where there is always a strong threat to soldiers in case of their presence. The damage of sensor nodes in that scenario is not noticeable because of their easily availability and inexpensive nature. As Wireless Sensor Networks (WSNs) have a vast variety of applications for military purposes, but keeping in mind the importance and critical nature of security and safety, there should be a number of more applications are possible in military operations. The proposed project is more secure and efficient to transfer data between users. This requires further research in this field.

REFERENCES

1. Ali Dorri, Seyed Reza Kamel and Esmail Kheyrkhah (2015) 'Security Challenges in Mobile Ad-hoc Network', Vol.6, No.1.
2. Dalimir Orfanus, Edison Pignaton de Freitas, and Frank Eliassen (2016) 'Self- Organization as a Supporting Paradigm for Military UAV Relay Networks', Vol.23, NO.2.
3. Du, X. (2014) 'QoS Routing Based on Multi-Class Nodes for Mobile Networks Ad- Hoc Networks', Vol. 2, pp. 241-254.
4. Hong Zhong, Lili Shao, Jie Cui (2016) 'A Light Weight and Secure Data Authentication Privacy'.
5. Ishfaq Ahmad, Khalil Shah, Saif Ullah (2016) 'Military Application Using Wireless Sensor Networks', Vol.6, No.6.
6. Reddy, T. Karthigeyan, I. Manoj, B. and Murthy, C. (2016) 'Quality of Service Provisioning in Wireless Networks: A Survey of Issues and Solutions', Ad Hoc Networks, Vol. 4, No. 1, pp. 83-124.
7. Saidivya, G. Rajendra, .C and Srilakshmi, A (2015) 'Secure Information Retrieval for Localized Disruption Tolerant Military Networks', Vol.5, No.7.
8. Sudipto Roy, Manisha Jnene, (2016) 'Analysis and Recommendations for Networks and Communication Security for Mission Critical Infrastructure'.