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

Ms. P. Suganthi malarvizhi[1], R. Manimozhi[2], S. Mythili[3], S. Pushpashree[4]

[1]Assistant Professor, Department of CSE, Velalar College of Engineering and Technology, TN, India.
[2, 3, 4] IV Year B. E., CSE, Department of Computer Science & Engineering,
Velalar College of Engineering & Technology, Erode, TN, India.

Received Date: 8th March, 2017, Revised Date: 19th March, 2017, Accepted Date: 4th April, 2017.

Abstract - Wireless Sensor Networks (WSN) are also called as wireless sensor and actuator networks. It is spatially distributed autonomous sensors to monitor physical or environmental conditions. It cooperatively passes their data through the network to the main location. WSNs received enormous attention in recent years due to its ability of implementation in various fields. WSNs consist of some small sensor nodes. These nodes are very cheap. In military operations, there is always a threat of being attacked by enemies. So, the use of these low-cost sensor nodes will help to reduce the loss. In this paper, we analyze the security of data transmission in WSNs for military applications. We will discuss the present scenarios of using sensor nodes in the armed uses. We aim to give a better deployment of sensor nodes for military purposes using cryptographic techniques. We will try to identify different areas and reduces the damage in militant's attack or enemy's outbreak using a brilliant deployment of nodes.

Keywords - Wireless Sensor Networks, MANET, DSRC, IBSS, FCC, ACC, DCF, AP, UAV.

I. INTRODUCTION

Military based Vehicular Ad hoc Networks are a subgroup of Mobile Ad hoc Networks (MANETs) with the property that the nodes are vehicles like cars, trucks, buses and motorcycles. This shows that node movement is restricted by factors like a road course, encompassing traffic and traffic regulations [3]. Due to the restricted node movement, the network will be supported by some fixed infrastructure that assists with some services. It can provide access to stationary networks. At critical locations for hazardous weather conditions the fixed infrastructure has to be deployed. Nodes are expected to communicate by using North American DSRC standard for wireless communication. Messages have to be forwarded by other nodes, to allow communication with participants out of radio range [4]. The vehicles are not subject to the strict energy, space and computing capabilities restrictions adopted for MANETs. Further challenging task is the potentially very high speed of the nodes (up to 250 km/h) and the large dimensions of the network.

The prime goal of the network is to increase road safety. To reach this goal, the vehicles act as sensors and can exchange warnings. It enables the drivers to react early to abnormal and potentially dangerous situations. The information provided by other vehicles and stationary infrastructure might also be used for driver assistant systems [1]. Also authorized entities like police or firefighters should be able to send alarm signals and instructions. Besides that, the network should increase comfort by using value-added services like the location based services or Internet on the road.

The various 802.11 wireless standards have caused a staged increase of wireless data networks. Today, wireless LANs are highly deployed. The cost for wireless equipment is continuing to drop in price. As a result of the high acceptance of the 802.11 standards, academia and the commercial sector in wireless technologies are looking for other applicable solutions. Mobile ad hoc networks are one area that has recently received considerable attention [5]. One hopeful application of mobile ad-hoc networks is the development of vehicular ad hoc networks.

A MANET is a self-forming network, which can function without the need of any centralized control. A data terminal and a router in ad-hoc network act as a node. The nodes in the network then use the wireless medium to communicate with other nodes in their radio range. A network is effectively a subset of MANETs [2]. The benefit of using ad-hoc networks is possible to introduce these networks in areas where it isn't feasible to install the needed infrastructure. Another advantage of ad-hoc networks is that they can quickly deploy without administrator involvement. The administration of a large scale vehicular set-up would be a difficult task. These reasons lead to the ad hoc network applied to vehicular environments. The Federal Communications Commission (FCC), realizing the problem of traffic fatalities. Dedicated Short Range Communication (DSRC) uses 5.9 GHz spectrum. The key goal is to enable the driver of a vehicle. To receive information about their surrounding environment vehicle's driver is enabled. To broadcast safety messages the control channel is used. The available services are broadcasted through the control channel. In control channel, if the vehicle finds a service of interest, then it switches to one of the service channels to use the service.

The creation of network has also spawned much attention in the rest of the world. Vehicular ad-hoc networks are also known under some different terms such as Inter-vehicle communication, Dedicated Short Range Communication or WAVE [6]. The purpose of most of these projects is to create new network algorithms. In the prospect vehicular ad hoc networks will help the drivers of vehicles and help to make safer roads by reducing the number of automobile accidents.

A. Challenges Creating AdHoc Networks

When constructing a vehicular ad hoc network, many challenges are addressed. One of the challenges facing ad-hoc networks is the topology of the network changes rapidly. Vehicles in a set of connections have a high degree of mobility.

It takes approximately one minute to calculate the average length of time that two vehicles are in direct communication range with each other[7]. Furthermore, wireless communication is unreliable. Ethernet has lower error rate than wireless networks. All of these issues make implementing a set-up difficult.

B. Media Access Control

The aim of media access control layer is to arbitrate the access to the shared medium. A huge number of collisions would occur and the data sent would be lost, If no method is used to coordinate the transmission of data. MAC is the best scenario that prevents nodes within transmission range of each other from transmitting at the same time, and no collision occurs.

To control the number of collisions and to reliably transmit packets with the use of CSMA/CD, the Distributed Coordination Function and the Point Coordination Function are the two protocols defined by 802.11 standards. The Distributed Coordination Function is a contention based access protocol. In a contention based protocol all nodes that have data to send content for the channel. It is easy to implement, but the problem with them is they offer no quality of service guarantees. Contention-free protocols are achieved by scheduling when a node can transmit. It enables the use of real-time services. The Point Coordination Function is a contention free protocol. It is not applicable to ad-hoc networks as it relies on the central node to support the real-time delivery of packets. One of the problems affecting the reliability of the DCF is the problem known as the hidden terminal problem and is shown in the Figure 1. The hidden terminal problem is the cause of collisions in a wireless network. Two nodes S1 and S2 cannot sense each other's transmissions. If both S1 and S2 were to transmit to R1 at the same time, a collision would occur.

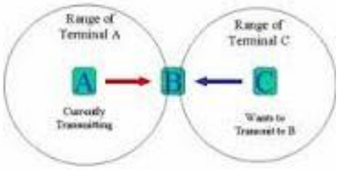

Fig. 1 Hidden Terminal Problem

II. RELATED WORKS

In literature survey, there exist various studies about implementing WSNs in military applications. Authors discussed these applications in various parts of military operations from altered perspectives. The various areas are pointed where WSNs deployed 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 attacks [2]. Intrusion Detection Sensor networks can be used as a 2-phase in Intrusion Detection System. Instead of using mines, an interruption can be spotted with the help of sensor network in a particular area. Mines can target the civilians as well as an alternative of mines; sensor nodes sense the environment and alarm the forces. Battlefield Surveillance Critical areas and borders can be monitored closely using sensor networks. This provides the quick gathering of information.

There are a variety of other applications of WSNs in military responsibilities. These include some of the above-mentioned areas while the other tasks for which these networks implemented are monitoring friendly forces, equipment, and ammunition and target. An advance in Group Filter Applications to Sea Mine Detection. It is extremely challenging to separate questions in the underwater environment which change in size, shape, and introduction from regularly happening and man-made disorder. Early attack reaction sensing element, Time difference of arrival blast localization using a network of disposable sensors [8], Novel optical sensor system for missile canisters continuous monitoring and Acoustic threatening sound recognition system are also included in the contents of the same paper. Tracking military vehicles, sniper localization and Self Healing Mine Field is also the portion of the existing study in the form.

The WSNs should be hidden and hard to abolish, in tracking military vehicles. For sniper localization, a WSN is being used to locate snipers and the trajectory of bullets, providing valuable clues for law enforcement. The deployment of Wireless Sensor Networks (WSNs) can solve the problem of enemy force deployment uncertainty. Where ever the force is deployed, sensor nodes will capture their presence and will inform. Then you have to send your army to that particular area to protect it. These networks can also be deployed in urban areas to make sure peaceful environment.

As discussed in above section, different authors discussed the applications of Wireless Sensor Networks (WSNs) for military purposes from different perspectives. In proposed system, the WSNs are used in battlefield surveillance to directly monitor the critical areas and borders to obtain information about enemy activity in that area. Hence, we will gather information quickly which will result in the quick response. The operations advance is another way of using sensor nodes for battlefield surveillance. Everyone has its advantages. Border monitoring is an essential component of military surveillance to prevent enemy's intrusion. In normal conditions, it may be enough just to monitor borders, but in the case of war, new sensor nodes are necessary to know the conditions of front areas so that you can adopt an appropriate plane. Nuclear, Biological and chemical (NBC) attack detection is an important application of Wireless Sensor Networks (WSNs). Nuclear, Biological, and Chemical agents are sensed by sensors, and embedded warning system can now send a caution message. It is good that can sense the NBC and can save many lives, but it should make sure that it can intellect the NBC even in a very tiny size and at very early stage. For this purpose, the sensor nodes can be placed close to these to the plant, and their threshold value should be set even very low then the danger limit therefore that preventive measures can be taken before the danger limit is reached. Tracking military vehicles is another important aspect of using sensors in military side. Here, sensor nodes are deployed from an unmanned aerial vehicle. To sense the closeness of tanks, Magnetometer sensors are attached to the nodes. To estimate the path and velocity of tracked vehicle Sensor nodes get collaborated. To track these vehicles, the tracking object should have a predefined amount of metallic material. This sum can be specified by the programmer while programming the sensor.

III. System Model

Two basic communication modes, which respectively allow nodes to communicate with each other, are used in our work and with the infrastructure RSUs. Since nodes communicate through wireless channels, a variety of attacks can occur. A security attack on a network can have severe harmful. A well-recognized solution to secure network is to deploy Public Key Infrastructure and to use Certificate Revocation Lists for managing the revoked certificate. In PKI, the network holds an authentic certificate in each entity and every message should be digitally signed before its transmission. A CRL, usually issued by a Trusted Authority, is a list containing all the revoked certificate. The authentication of any message is performed by first checking the sender's certificate whether it is included in the current CRL in a PKI system. i.e., checking its revocation status, then, Certificate of the sender is verified, and finally signature of the sender is also verified on the received message.

Elliptic Curve Integrated Encryption Scheme (IES) is a public key encryption scheme. The ECIES functions are defined in huecc.h. ECIES is a hybrid encryption scheme. It provides semantic security. The scheme is based on the Diffie–Hellman problem. Two qualities of the IES are standardized: Discrete Logarithm Integrated Encryption Scheme and Elliptic Curve Integrated Encryption Scheme. These two qualities are identical up to the change of an underlying group. It combines a Key Encapsulation Mechanism (KEM) with a Data Encapsulation Mechanism (DEM). A bulk encryption key is derived from system independently and a MAC key from a common secret. Data is first encrypted with a symmetric cipher, and then the ciphertext is MAC ID under an authentication scheme. Finally, the common secret is encrypted under the public part of a public/private key pair. The tuple {K, C, T}, where K is the encrypted common secret, C is the cipher text, and T is the authentication tag are the output of the encryption function. There is some hand using the "common secret" since it's actually the result of applying a Key Agreement function. It uses the static public key and an ephemeral key pair. Elliptic Curve Integrated Encryption Scheme operates on elliptic curves, while Discrete Logarithm Integrated Encryption Scheme operates on integers.

Since the development of public key cryptography by Diffie and Hellman in 1976, several cryptosystems have published. In particular, Miller and Koblitz proposed in 1985 a cryptosystem whose security relies on the Elliptic Curve Discrete Logarithm Problem. So extreme, no algorithm is known that solves the ECDLP in an efficient way, and some authors consider that this mathematical problem is more difficult to solve other mathematical problems which are used in other cryptosystems. This is the reason why the key length in ECC is significantly smaller than in other cryptosystems as RSA, which presents a comparison of key lengths associated with the same cryptographic strength for RSA and ECC, where the cryptographic strength is interpreted. The security level provided by a symmetric encryption algorithm using a key of n bits.

IV. Skipjack based 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 be 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.

Algorithm to sign a message M:

1) choose a random number k, m is message, g no of digits in random number, p is no of digits in message
2) compute $a = gk(\mathrm{mod}\ p)$
3) use extended Euclidean algorithm to solve $b = m.g + m.p$
4) the signature is (a, b) and k must be kept secret
5) to verify a signature (a ,b), the algorithm need to be reversed.

V. Conclusion

From the above discussion, it is clear that WSNs plays an important role in military applications. With the help of these WSNs, 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. In addition, due to its fault tolerance characteristic, if any node got damaged, the rest of the network will continue sensing. Due to the damage of a single or a group of sensors rest of the network will not be affected. The use of 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 the case of their presence. The damage of sensor nodes in that scenario is not noticeable because of their easy availability and inexpensive nature. As discussed prior, 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 some more applications are possible in military operations. This requires further research in this field.

REFERENCES

[1] P. Papadimitratos, A. Kung, J.P. Hubaux and F. Kargl, “Privacy and Identity Management for Vehicular Communication Systems: A Position Paper,” Proc. Workshop Standards for Privacy of User- Centric Identity Management, July 2006.

[2] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura and K. Sezaki, “CARAVAN: Providing Location Privacy for VANET,” Proc. Embedded Security in Cars (ESCAR) Conf, Nov 2005.

[3] A. Wasef, Y. Jiang and X. Shen, “DCS: An Efficient Distributed Certificate Service Scheme for Vehicular Networks,” IEEE Trans. Vehicular Technology, vol. 59, no. 2 pp. 533-549, Feb 2010.

[4] M. Raya and J.P. Hubaux, “Securing Vehicular Ad Hoc Networks,” J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[5] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, “An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications,” IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept 2010.

[6] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, “Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETS,” IEEE Trans. Vehicular Technology, vol. 61, no. 1, pp. 86-96, Jan 2012..

[7] J.J. Haas, Y. Hu and K.P. Laberteaux, “Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET,” Proc. Sixth ACM Int’l Workshop Vehicular InterNETworking, pp. 89-98, 2009.

[8] IEEE STD 1609.2-2006, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE, 2006..