Providing Mutual Authentication and Light Weight Encryption Schema in Mobile Adhoc Network

BhagyaRaju Sanchana¹, Chintada Sunil Kumar ²
¹Final M.Tech Student, ²Asst.professor
¹,²Dept of CSE, Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh

Abstract:
Mobile Ad Hoc Networks (MANETs) are important wireless communication paradigms. The mobile and infrastructure less nature of MANETs makes them suitable for collecting emergency data in disastrous areas and performing mission-critical communication in battle fields. A critical issue in MANETs is how to reduce energy consumption and maintain a longer life time for mobile nodes. In this paper we are proposed mainly two concepts for performing mutual authentication of each user in the mobile adhoc network and other concept for performing encryption and decryption of transferring data. Before performing encryption and decryption of data each user will perform the mutual authentication. After that each node will exchange data using data exchange protocol. By considering those concepts we can provide less time complexity for data encryption process and also improve network efficiency. Because by implementing proposed system we can provide light weight encryption process and also reduce number of keys usage in the network. In this paper we can also implement the mutual authentication of each user in the network. By implementing this concept we can reduce time complexity for authenticating each node in the mobile adhoc network. So that by implementing those concepts we can reduce number of keys and also improve efficiency of mutual authentication of node.

Keywords: Encryption and Decryption, Symmetric keys, mutual authentication, security, data exchange

I. Introduction

MOBILE Ad Hoc Networks (MANETs) are very important wireless communication. Mobile ad hoc networks (MANETs) is an infrastructure less, dynamic network consisting of collection of wireless mobile nodes that communicates with each other without the use of any centralized authority. Mobile ad hoc network is now becoming interesting research topic in the area of wireless communication. Vehicles in the particular range from a network to communicate with each other without any need of a base station. MANET provide comfort and safety applications such as lane changing, traffic sign violation, weather information, road condition, location of restaurants or fuel station, parking and interactive communication such as internet access [2]. As shown in figure 1 MANET provides multiple services, energy is required. Thus, energy saving is an important issue in Mobile ad hoc network. There are several energy efficient schemes used to overcome this problem [3], [4] and [5]. Many researchers show that network coding can reduce energy consumption in MANET with less transmission [6]. Network coding can be defined as coding performed at a node in a network, where coding means casual mapping from inputs to outputs. Idea behind it is to mix and forward data to output links [7]. A node in the network encodes the packet with the network coding and then forwards it to another node. Network coding requires less energy for this process of encoding. Figure 2 clarify the use of network coding in ad hoc network. Suppose there are six nodes forming hexagon and transmission range of each node reaches to its right and left neighbor. Each message would require four transmissions without network coding. When network coding is used for three messages the total number of nine transmissions are needed, i.e., three transmissions per message. It would save ¼ energy without considering energy required for the process of encryption and decryption.

Mobile ad hoc network is the network which provides seamless connectivity between devices when they move with their neighbor wireless nodes. For sending packets it does not have any access point and routers. In a MANET each device is free to move independently, and so it can frequently change its link at any time. MANETs nodes can communicate directly between each other so that MANETs can emerged as a dominant mode of communication at any place. Some of the characteristics of MANETs includes infrastructure-less network, dynamic network topology and self-organization etc. In ad hoc networks all nodes are responsible for running the network services meaning that every nodes are also works as a router to forward the networks packets to their destination. Data communication in a MANET differs from that of wired networks in different aspects. The bandwidth availability and computing resources like hardware and battery power are restricted in mobile ad hoc networks. An ad hoc network is a decentralized type of wireless network. The ad hoc
network is the network that links with each other for communication having fixed infrastructure. It is made up of multiple nodes connected by links. A MANET can be created either by mobile nodes or by both static and dynamic mobile nodes. Mobile ad hoc network is created by cluster of is a form of a Mobile Ad Hoc Network (MANET) is formed.

II. RELATED WORK

There are two main keying protocols that were proposed in the past to reduce the number of stored keys in each sensor in the network. We refer to these two protocols as the probabilistic keying protocol and the grid keying protocol. In the probabilistic keying protocol [4], each sensor in the network stores a small number of keys that are selected at random from a large set of keys. When two adjacent sensors need to exchange data messages, the two sensors identify which keys they have in common then use a combination of their common keys as a symmetric key to encrypt and decrypt their exchanged data messages. Clearly, this protocol can probabilistically defend against eavesdropping. Unfortunately, the probabilistic keying protocol suffers from the following problem. The stored keys in any sensor x are independent of the identity of sensor x and so these keys cannot be used to authenticate sensor x to any other sensor in the network. In other word, the probabilistic protocol cannot defend against impersonation.

In the grid keying protocol [5], [6], [7], and [8], each sensor is assigned an identifier which is the coordinates of a distinct node in a two-dimensional grid. Also each symmetric key is assigned an identifier which is the coordinates of a distinct node in a two-dimensional grid. Then a sensor x stores a symmetric key K if the identifiers of x and K satisfy certain given relation. When two adjacent sensors need to exchange data messages, the two sensors identify which keys they have in common then use a combination of their common keys as a symmetric key to encrypt and decrypt their exchanged data messages. The grid keying protocol has two advantages (over the probabilistic protocol). First, this protocol can defend against impersonation (unlike the probabilistic protocol) and can defend against eavesdropping (like the probabilistic protocol). Second, each sensor in this protocol needs to store only O(\log n) symmetric keys, where n is the number of sensors in the network. Unfortunately, it turns out that the grid keying protocol is vulnerable to collusion. Specifically, a small gang of adversarial sensors in the network can pool their stored keys together and use the pooled keys to decrypt all the exchanged data messages in the sensor network. This situation raises the following important questions: Is it possible to design a keying protocol, where each sensor stores less than n-1 symmetric keys and yet the protocol is deterministically secure against impersonation, eavesdropping, and collusion.

The remaining concepts of this paper are as follows. Section 2 is to specify related work of our proposed system. Section 3 implementation procedure of our proposed system. Section 4 is conclusion of our proposed system. Section 5 is reference of can be specify in this paper.

III. PROPOSED SYSTEM

In this paper, system describe in MANET Energy saving & security in data is an important issue in MANET. This can be solved by network coding which might reduce energy consumption also by using less transmission this system proposed data sharing using data encryption method. Encryption/decryption cost along with transmission time is factor of energy consumption in wireless network. In MANET unreliable wireless media, mobility, lack of infrastructure is a big challenge. Let n denote the number of sensors in our network. Without loss of generality, we assume that n is an odd positive integer. Each sensor in the network has a unique identifier in the range 0 : : : n-1. We use ix and iy to denote the identifiers of sensors x and y, respectively, in this network. Each two sensors, say sensors x and y, share a symmetric key denoted Kxy or Kyx. Only the two sensors x and y know their shared key Kxy. And if sensors x and y ever become neighbours in the network, then they can use their shared symmetric key Kxy to perform two functions:

1) Mutual Authentication: Sensor x authenticates sensor y, and sensor y authenticates sensor x.
2) Confidential Data Exchange: Encrypt and later decrypt all the exchanged data messages between x and y. (Note that sensors x and y can become neighbours in the network in two occasions. First, the two sensors x and y could be mobile and their movements cause them to become adjacent to one another. Second, the two sensors could be stationary and they are deployed adjacent to one another.)

In the remainder of this section, we show that if the shared symmetric keys are designed to have a “special structure”, then each sensor needs to store only \((n+1)\times 2\) shared symmetric keys. But before we present the special structure of the shared keys, we need to introduce two new concepts: “universal keys” and “a circular relation, named below, over the sensor identifiers”.

Each sensor x in the network stores a symmetric key, called the universal key of sensor x. The universal key of sensor x, denoted ux, is known only to sensor x. Let ix and iy be two distinct sensor identifiers. (Recall that both ix and iy are in the range 0 : : : n-1, where n is the odd number of sensors in the sensor
After every sensor is authenticated, sensor y concludes that the sensor and sensor x proves to sensor y that it is indeed sensor x. Otherwise, no conclusion can be reached.

Step 5: Sensor y computes \( H(iy|ix|ny|K_{x;y}) \) and compares it with the received \( H(iy|ix|ny|K_{y;x}) \). If they are equal, then y concludes that the sensor claiming to be sensor x is indeed sensor y. Otherwise, no conclusion can be reached.

A DATA EXCHANGE PROTOCOL:

After two adjacent sensors x and y have authenticated one another using the mutual authentication protocol described in the previous section, sensors x and y can now start exchanging data messages according to the following data exchange protocol. (Recall that nx and ny are the two nonces that were selected at random by sensors x and y, respectively, in the mutual authentication protocol.)

Step 1: Sensor x concatenates the nonce ny with the text of the data message to be sent, encrypts the concatenation using the symmetric key \( K_{x;y} \), and sends the result in a data message to sensor y.

\[
x \rightarrow y : \text{data}(ix, iy, K_{x;y}(ny|text))
\]

Step 2: Sensor y concatenates the nonce nx with the text of the data message to be sent, encrypts the concatenation using the symmetric key \( K_{x;y} \), and sends the result in a data message to sensor x.

\[
x < \rightarrow y : \text{data}(iy, ix, K_{x;y}(nx|text))
\]

Sensors x and y can repeat Steps 1 and 2 any number of times to exchange data between themselves.

IV. CONCLUSIONS

Typically, each sensor in a sensor network with n sensors needs to store (n-1) shared symmetric keys to communicate securely with each other. Thus, the number of shared symmetric keys stored in the sensor network is \( n(n-1) \). However, the optimal number of shared symmetric keys for secure communication, theoretically, is \( n(n-1)/2 \). Although there have been many approaches that attempt to reduce the number of shared symmetric keys, they lead to a loss of security: they are all vulnerable to collusion. In this paper, we show the protocols for sensor networks, that needs to store only \( n+1 \) symmetric keys to each sensor. The number of shared symmetric keys stored in a sensor network with n sensors is \( n(n+1)/2 \), which is close to the optimal number of shared symmetric keys for any key distribution scheme that is not vulnerable to collusion. It may be noted that in addition to the low number of keys stored, and the
ability to resist collusion between sensors, our keying protocol has two further advantages. Firstly, it is uniform: we store the same number of keys in each sensor. Secondly, it is computationally cheap, and thus suitable for a low-power computer such as a sensor: when two sensors are adjacent to each other, the computation of a shared symmetric key requires only hashing, which is a cheap computation and can be done fast. As our protocol has many desirable properties, such as efficiency, uniformity and security, we call this protocol the best protocol for sensor networks.

V. REFERENCES


BIOGRAPHIES:

Bhagyraju Sanchana is student in M.Tech (CSE) in Sarada Institute of Science Technology and Management, Srikakulam, Andhra Pradesh. He has received his B.Tech(CSE) GMRIT, Rajam, Srikakulam. His interesting areas are network security, image processing and web technologies.

Chintada Sunil Kumar working as a Asst Professor of CSE in Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh. He received his M.Tech (CSE) from Jntuk, Kakinada, Andhra Pradesh. His interest research areas are Database management sysytems,Computer Architecture, Image Processing, Computer Networks, Distributed Systems. He published 4 international journals and he was attended number of conferences and workshops.