Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Unique light weight time stamp based Security Protocol for Wireless Adhoc Network

Juli
M.Tech. Scholar, Computer Science & Engineering
AL-Falah School of Science & Technology
Dhauj, Faridabad, India

Ms. Manisha Dawra
Asst. Professor, CSE Deptt
AL-Falah School of Science & Technology
Dhauj, Faridabad, India

Abstract — In MANET strong encryption algorithms are difficult to implement due to computational complexity. Therefore authentication along with encryption is to be used with different variants suitable to the specific network. As there are no central base station authentication is difficult to implement. Hence oblate public key cryptography is most prominently being used.

1. ***It is transmitting emergent data to the based station;***
2. ***The proposed scheme can also resist altering, forging and dropping attacks.***
3. ***In the future, I will focus on reducing the overhead of Computation cost.***
4. ***In addition, I will aim to provide better security to resist other attacks.***

Once a wireless system is installed, the user owns the medium, and there are no ongoing charges for communications. The equipment costs for a wireless link are often recovered within a very short time. Network security is another concern with hardwired systems. Because cables are vulnerable to accidental or intentional damage, it is nearly impossible to ensure the integrity of the network. While no system can be 100% secure.

Keywords: Introduction, Concept and Explanation, Methodology/planning of work, Security Enhancement of Pro-active Protocols in Mobile Ad-hoc, Lightweight User Authentication Protocol, Conclusion.

I. INTRODUCTION

In MANET strong encryption algorithms are difficult to implement due to computational complexity. Therefore authentication along with encryption is to be used with different variants suitable to the specific network. As there are no central base station authentication is difficult to implement. Hence oblate public key cryptography is most prominently being used.

Wireless network may be configured either as a infrastructure network or infrastructure less network and the devices in the network communicated using IEEE 802.1x MAC standard. IEEE802.11 provides security to the packets transmitted over the network using two conventional techniques viz Authentication and Encryption. For authentication purpose, a node is configured as special radius server. Encryption is implemented through wireless encryption protocol (WEP) which comes with 802.11 protocol suite. The attacks are categorized into two major categories viz: Session hijacking attack which is a scenario where by an intermediate unauthenticated node attacks the packet and this is applicable where encryption is disabled. The attacker waits until the authentication is completed. Once the authentication is completed, it issues a disassociate message to the client and transmits data through the valid access point. On the contrary in the second type, Man in the middle attack, an intrusive node places itself between two valid devices and intrudes the packet exchanged between them. Authentication with strong encryption algorithm like that in the case of IEEE802.11i is the most adopted algorithm for wireless security purpose. The basic problem with the existing protocol is extensive amount of data exchange for authentication and requirement of excessive processing power for strong encryption techniques. Both of these leads to bandwidth consumption and subsequently delay in initial packet transmission, and excessive energy loss due to higher processing cycles for encryption. Therefore the devices which are purely battery driven and for those network which are without any centralized control, achieving a tradeoff between packet security with keeping the energy losses and bandwidth consumption minimum is a challenge far beyond the issue of selecting the most appropriate protocol. More security invariably increases the latency, whereas less strong encryption mechanism results in more eavesdropping. In order to have a balance between the security and performance, generally either the quality of transmission is sacrificed or strength of the key is satisfied or the encryption mechanism is compromised. Moreover in any technique, it is suggested that the key used for encryption be refreshed periodically (at least once in every 30 minutes). In this work we propose a unique technique for achieving secured data transmission in wireless infrastructure less network which attains high security with minimum compromise with the quality of service of transmission.

II. CONCEPT AND EXPLANATION

1. The node exchange hello message at the start of the network or session to build the routing table or neighbor table.
2. We propose a new hello packet structure where a node appends transmission timestamp in the hello packet and broadcast the hello packet.

3. Each node notes down its transmission timestamp for the hello packet.
4. Once the hello packet is received by the node, it makes a routing table entry for the sender node. We device a time stamp based hash generation technique. Once all the nodes receiving the hello packets from the sender node, makes a table entry of the sender nodes id and the transmission time stamp. This time stamp acts like the public key between the sender and the receiving nodes. When the sender intern receives the hello packet from all these nodes which had received hello packet transmitted by the sender, sender also makes a table entry of these nodes and corresponding time stamps. Therefore in a session there is a single pair of base function for generating the key between any two nodes.
5. Now we assume that a node joins right at the middle of hello message exchange and acquires the time stamp values of the neighboring nodes. If this node is not an authenticated node, it will not be preloaded with the hash generation method and needs time for guessing the hash in the course of any data exchange between valid nodes. Hello interval in adhoc network is generally kept at three seconds. Hence in every three seconds the base pair between any two nodes gets changed thus making it impossible for the intruder to guess the hash.
6. Another type of threat that might occur in the network is that an unauthenticated person gets access of a valid device of the network and hacks the data even being unauthenticated. In a centralized system this problem is solved through authentication protocol. In authentication protocol, the user enters his authentication information like username and password which upon matching with a central storage, the system authenticates the user and the device can subsequently take part in the communication. In a decentralized method such authentication

III. METHODOLOGY / PLANNING OF WORK

Once a wireless system is installed, the user owns the medium, and there are no ongoing charges for communications. The equipment costs for a wireless link are often recovered within a very short time. By contrast, the difficulty of installing and maintaining leased lines makes their cost very high. This is particularly true in high bandwidth applications, such as the transmission of video. The cost of video-capable lines can easily exceed $300 per month.

Network security is another concern with hardwired systems. Because cables are vulnerable to accidental or intentional damage, it is nearly impossible to ensure the integrity of the network. While no system can be 100% secure, MDS wireless solutions offer an inherently more secure infrastructure, as there are no cables exposed to possible damage, sabotage or tapping by unauthorized persons. MDS Wireless systems replace the wired infrastructure with an over-the-air RF link, allowing immediate, reliable communication with remote sites at ranges up to 30 miles. More is said about cyber security in a white paper about the MDS iNET 900

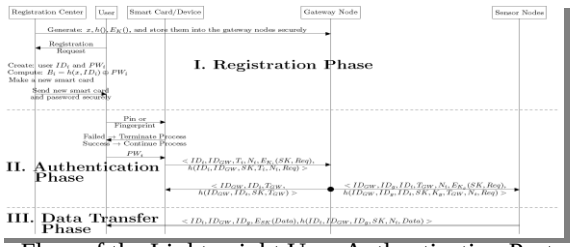
IV. SECURITY ENHANCEMENT OF PRO-ACTIVE PROTOCOLS IN MOBILE AD-HOC

The most demanding technology now days are Mobile Ad Hoc Networks (MANETS). Ad hoc wireless network consists of nodes which communicate with other nodes through wireless medium without any fixed infrastructure. In this figure there are three nodes in the network, source node, intermediate node and destination node. Each node worked as peer-to-peer mode and considers as independent router and generates independent data. In author describes the characteristics of mobile ad-hoc networks. Ad-hoc network topology is dynamic, self-organization, and self-administration. Network topology changes at any time by entering or leaving of node. Due to high mobility of nodes the network topology may change quickly and unpredictably.

There is no central entity in Ad-hoc wireless network, so nodes have to discover the topology and deliver the messages generated by all nodes. It is a multi-hop wireless network with limited physical security. In a node can use multi-hops to transmit a data from source to the destination. There is no default router or node present so each node works as router and transmit packets to other nodes to enable information sharing between mobile nodes. There are three main components or resources of node are battery, memory, and computation. Batteries present in each mobile node limit processing power so battery life should be better especially in war scenarios. This is the worst problem in MANETs because a node performs the duties as end system and router. Additional energy is required to forward packets from other nodes. Ad–hoc wireless network is scalable. In network topology all nodes broadcast Hello massages in the network topology to get information of their neighboring nodes while signaling period

V. LIGHTWEIGHT USER AUTHENTICATION PROTOCOL

1. Lightweight User Authentication Protocol : The lightweight user authentication protocol we propose is based on smart card technology. The smart card can be integrated into the user's mobile devices with self-lock or destroy functionality for physical security. The protocol uses a hash to protect the system secret and consists of three phases: registration, authentication, and secure data transfer phases. Figure 3 depicts the data flow of the lightweight user authentication protocol



Data Flow of the Lightweight User Authentication Protocol

A. Registration Phase:-

The system generates the following parameters: x, $h()$, and $E_K()$, and stores them into the gateway nodes, where x is the system secret. The registration center creates a user identity ID_i and remote access password PW_i, computes a long-term key K_i as $K_i=h(x, ID_i)$ and $B_i=K_i \oplus PW_i$ for user U_i, stores ID_i, B_i, $h()$, and $E_K()$ onto a new smart card, and sends the smart card with the password to the user in a secure way. The user knows nothing about the system secret x and K_i if he does not compromise his smart card physically and extract the parameter B_i but can change passwords after receiving the smart card.

For password change, the smart card needs to update the data B_i stored in the card by $B_i'=B_i \oplus PW_i \oplus PW_i'$, where PW_i is the old password and PW_i' is the new password. To do this, the protocol has two options. The first option does not require connecting to the registration centre. In it, the user needs to connect to the registration centre to re-setup his password if he inputs an incorrect one. The second option is that the user needs to go through the following authentication procedure and let the gateway node verify his old password first.

B. Authentication Phase:-

The authentication phase contains the following three steps.

Step 1: The user U_i inserts his smart card into his mobile device and keys a pin or scans his finger for smart card access authentication. If the pin or fingerprint verification is successful, the user then keys the remote access password. Unlike the strong user authentication, the smart card authenticates the user with the pin or fingerprint but not the remote access password for smart card access. This can provide another security feature such as stealing and compromising the smart card since we do not directly store the remote access password and system secret in the card.

The smart card recovers the user's long term key K_i by $K_i=B_i \oplus PW_i$, and sends the following request message to the gateway node GW:

Message 1. $U_i \rightarrow GW$:

$$<ID_i, ID_{GW}, T_i, N_i, E_{Ki}(SK, Req), h(ID_i, ID_{GW}, SK, T_i, N_i, Req)>,$$

where T_i is the current timestamp of U_i's device, SK is a session key generated by the smart card.

Step 2: Upon receiving the request message at time T_{GW}*, the gateway node GW validates the destination identity ID_{GW} and the timestamp T_i by comparing T_{GW}*-$T_i \leq \Delta T$. If the verification is successful, GW recovers the user's long-term key K_i by $K_i=h(x, ID_i)$ and decrypts the cipher text with K_i. It then validates the user and received message by checking the hash value. If they are correct, it sends the following authentication message back to the smart card:

Message 2. $GW \rightarrow U_i$:

$$<ID_{GW}, ID_i, T_{GW}, h(ID_{GW}, ID_i, SK, T_{GW}, Req)>,$$

where T_{GW} is the current timestamp of the gateway node.

Meanwhile, the gateway node sends the following message back to the targeted sensor nodes:

Message 3. $GW \rightarrow S_g$:

$$<ID_{GW}, ID_g, ID_i, T_{GW}, N_i, E_{Kg}(SK, Req), h(ID_{GW}, ID_g, ID_i, SK, K_g, T_{GW}, N_i, Req)>.$$

where K_g is the group key of the sensor nodes having the requested data, ID_g is their group identity, T_{GW} is the current timestamp of the gateway node. K_g is managed by the gateway and could be updated periodically depending on the different applications. K_g could be also a shared key between the gateway node and a specific sensor node under the situation when the requested data only is stored on that sensor node. For key management among sensor nodes and GWs such as group key and shared key establishment, we can use existing technologies (e.g., IKDM [17] and Key Evolution [18]), which is beyond the scope of this paper.

Step 3: After receiving the authentication message $<ID_{GW}, ID_i, T_{GW}, h(ID_{GW}, ID_i, SK, T_{GW}, Req)>$ at time T_i*, the smart card validates the destination identity ID_i, the timestamp T_{GW} by comparing T_i*-$T_{GW} \leq \Delta T$, and the received message by checking the hash value. If the authentication is successful, it waits for the data from the sensor nodes.

C. Secure Data Transfer Phase:-

Upon receiving the message sent by the gateway node at time T*, the sensor nodes check the group identity ID_g and validate the timestamp T_{GW} by T*-$T_{GW} \leq \Delta T$. The sensor nodes decrypt the cipher text with the group key K_g and validate the received message by checking the hash value. If the authentication is successful, the sensor nodes send the requested data to the user through the following secure channel:

Message 4. $S_g \rightarrow U_i$:

$$< ID_g, ID_i, ID_{GW}, E_{SK}(Data), h(ID_g, ID_i, ID_{GW}, SK, N_i, Data)>.$$

The user decrypts the data with the session key SK after receiving the message from the sensor nodes and validates the received message by checking the hash value.

D. *Cryptography will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The types of algorithms are three that is explain in figure given below.*

1. Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
2. Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
3. Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

VI. CONCLUSION

I proposed a lightweight secure data aggregation protocol for Time Stamp based Security protocol for Wireless Adhoc Network. Besides transmitting emergent data to the based station, the proposed scheme can also resist altering, forging and dropping attacks. The proposed scheme can effectively detect the attacker. I also provide the security analysis and the simulation results to justify that the proposed scheme can resist attacks effectively and efficiently. In the future, I will focus on reducing the overhead of computation cost. In addition, I will aim to provide better security to resist other attacks

REFERENCES

[1] F. Baker, "An outsider's view of MANET," Internet Engineering Task Force document, 17 March 2002.
[2] C. Barrett et al., "Characterizing the Interaction between Routing and MAC Protocols in Ad-hoc Networks," *Proc. MobiHoc 2002.*
[3] J. Broch et al., "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," *Proc. Mobicom '98*.
[4] M. S. Corson et al., "Internet-Based Mobile Ad Hoc Networking," *IEEE Internet Computing*, July-August 1999.
[5] L. M. Feeney, "A Taxonomy for Routing Protocols in Mobile Ad Hoc Networks," Swedish Institute of Computer Science Technical Report T99/07, October 1999.
[6] S. Kurkowski, et al., "MANET Simulation Studies: The Incredibles," *ACM SIGMOBILE Mobile Computing and Communication Review*, Vol. 9, Issue 4 (October 2005).
[7] C. E. Perkins, *Ad Hoc Networking*. New York: Addison-Wesley, 2001.

