Mobile Ad-hoc Network – A Novel Node Authentication Mechanism

Syed Azhar Mahmood[1], Farhan Ahmed[2], Zaffar I. Qureshi[3], M.N.Jafri[4]
Information Security Department, College of Signals[1, 3]
Electrical Engineering Department, College of Signals[4]
National University of Science & Technology
Tamizuddin Road, Rawalpindi, Pakistan
Computer Science Department[2]
University of Kakul, Abbottabad, Pakistan

Abstract: Mobile ad-hoc network **(**MANET**)** is a kind of wireless ad-hoc network. It is a self-configuring network of mobile nodes connected by wireless links, without the aid of any fixed infrastructure or centralized administration. Nodes within their wireless transmitter ranges can communicate with each other directly, while nodes outside the range rely on other nodes to relay messages resulting in a multi-hop scenario. As the low transmission power of each node limits its communication range, the nodes must assist and trust each other before getting involved into a real communication. However, this implied trust relationship can be threatened by malicious nodes. So far the majority of research work has been done to achieve a secure routing infrastructure, assuming the existence of an efficient node authentication mechanism which in turn is part of a key management scheme. This paper will analyze previous work and then present a new node authentication mechanism which is fully distributed and has the ability to self-organize with out the requirement of any online trusted third party.

Key-Words: *Mobile ad-hoc networks, public key, secret key, private key, check word.*

1. Introduction

A mobile ad-hoc network (MANET) is a communication network whose topology can change over time, due to both, node mobility and limited node energy. The fact that MANETs does not rely on any fixed infrastructure [6], [7], [8], [9] gives them several advantages over conventional networks; namely that the setup time is small, which is ideal for applications such as war zone surveillance/communication, or disaster zone search-and-rescue missions where rapid deployment is necessary. MANETs also suffer from several disadvantages, including limited communication range, battery life, and only local knowledge of their environment. This lack of infrastructure makes necessary for a MANET to be self organizing, and the lack of global knowledge requires a distributed control policy [1].

Authentication is one of the major security issues affecting the wired and the wireless network community [5]. It is generally accomplished in two ways: direct and indirect authentication. In direct authentication, two parties use pre-shared symmetric or asymmetric keys for verifying each other and the flow of data between them. In indirect authentication, a trusted third party, i.e. a certification authority, is made responsible for certifying one party to another party. Most of the secure routing protocols developed for MANETS rely on indirect authentication mechanisms using public key infrastructures (PKI) to authenticate communicating nodes. PKI is although a secure system based on asymmetric cryptography, but requires excessive processing and communication resources [2].

2. Analysis of Previous Work

The previous work is analyzed with a view to find out different weaknesses in relation to node authentication mechanism.

2.1 Distributed Public-Key Model

The distributed public-key model [11] makes use of threshold cryptography to distribute the private key of the certification authority over a number of servers. An (n, t+1) scheme allows any t+1 servers out of a total n servers to combine their partial keys to create the complete secret key. Similarly it requires that at least t+1 servers be compromised to acquire the secret key [2], [9].

2.1.1 Observations

The discussed scheme seems quite robust but has a number of limitations, limiting its implementation to MANET. The first observation relates to the fact that under all circumstances, it might not be possible for a node to access specific number of servers desiring authentication at any particular instance. Secondly, in case of asymmetric cryptography, cryptographic operations are known to drain precious node batteries due to heavy mathematical computations.

2.2 Password-Based Key Agreement

The work developed refers to a scenario of a group of people who want to set up a secure session in a meeting room without any support infrastructure. A weak password is sent to the group members. Each member then contributes part of the key and signs this data by using the weak password. Finally a secure session key to establish a secure channel is derived without any central trust authority or support infrastructure. The problem is that only those entities that know an initial password are authentic nodes and only they are able to learn the session key. Perfect forward secrecy requires that an attacker who compromises one member of the group and learns all his permanent secret information is still unable to recover the session key [3].

2.2.1 Observations

This model seems perfect for small groups desirous to become a part of MANET as authentication is done outside the premises of an information technology (IT) system. The group members authenticate themselves by showing their passports or based on common knowledge and common technique but the model is inadequate for more complicated environments. An example to this can be groups of people who do not know each other or two persons who want to communicate confidentially without the rest of the persons in a group to eavesdrop on the channel.

2.3 Self- Organized Public Key Management

In contrast with conventional networks, MANETs usually do not provide on-line access to trusted authorities or to centralized servers and they exhibit frequent partitioning due to link and node failures and to node mobility. For these reasons, traditional security solutions that require on-line trusted authorities or certificate repositories are not well suited for securing ad hoc networks. Fully self-organized public-key management system allows users to generate their public-private key pairs, to issue certificates, and to perform authentication regardless of the network partitions and without any centralized services. Furthermore, this approach does not require any trusted authority [4].

2.3.1 Observations

Requirement of huge memory space for storage of local repositories is a big drawback in this model as in case of the mobile nodes limited storage capacity is available. Small hand held portable devices with limited memory can be a good example of this fact. The other problem of public-key based security system secure distribution of each user’s public key to others in such a way that its authenticity is provable.

2.4 PGP Model

In the pretty good privacy model [10] all users act like independent certification authorities and have the capability to sign and verify keys of other users. PGP breaks the traditional central trust authority architecture and adopts a decentralized “web of trust” approach. Each individual signs each other’s keys that help build a set of virtual interconnecting links of trust. PGP attaches various degrees of confidence levels from “undefined” to “complete trust” to the trustworthiness of public-key certificates and four levels of trustworthiness of introducers from “don’t know” to “full trust”. Based on these trust levels the user computes the trust level of the desired party [2].

2.4.1 Observations

PGP is suitable for a wired network where a central key server can maintain a database of keys but for MANETs, a central key server creates a single point of failure. Furthermore, uninterrupted access by nodes to the central key server can not be assured.

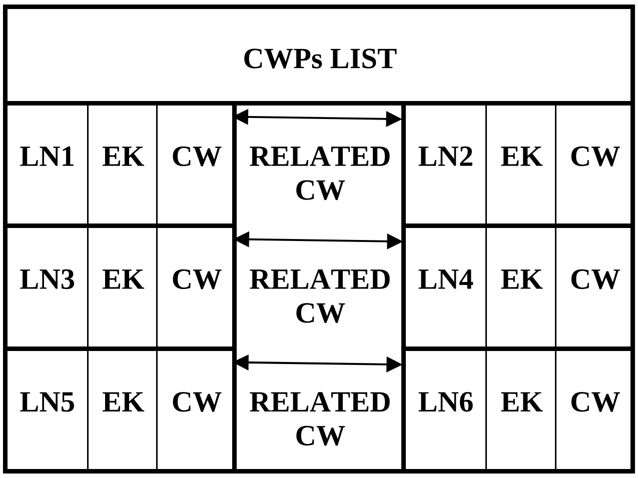
3. New Node Authentication Mechanism

After analyzing the previous work, we are now proposing a new node authentication mechanism in MANETs. It is able to self organize itself and does not require any additional network infrastructure like online central authority, key distribution centre or trusted third party. Moreover, it is capable of handling the dynamic network topology requirements of MANETs. Also, if a node is compromised and resultantly gets into the hands of an unauthorized person, he will not be able to easily use the node or extract any information out of it.

3.1 Assumptions

In this technique, we have assumed following:-

- Each node should be able to store sufficient number (approximately 40) of encrypted check word pairs (CWPs). The proposed composition of CWP is shown in Figure 1.



CWPs LIST						
LN1	EK	CW	RELATED CW	LN2	EK	CW
LN3	EK	CW	RELATED CW	LN4	EK	CW
LN5	EK	CW	RELATED CW	LN6	EK	CW

Figure 1: Composition of CWPs

- Each node must be able to store sufficient communication encryption keys (CEKs) (approximately 40) in encrypted form.
- System clocks for loose synchronization.
- Each node must have a unique ID (can be its MAC address) and the Private Key (VK).
- Each node must have a directory comprising of IDs of all nodes included in the friends list, along with their Public Keys (PK).
- A controlling program which is capable of shuffling the entries of CWPs and CEKs after a pre-defined time interval and in a predefined order. This shuffle will remain same for all the nodes. This program will also allow the nodes to calculate, implement and transmit the secret key (E) after a time interval $t_{E.}$input. Therefore, E will also change after every $t_{E.}$ The program will also have the provision of calculating all the changes to the CEK and CWP by giving the first launch time and the current time in order to allow a new node to join the MANET.

3.2 Notations Table

ID_a	ID of node **a**
VK_b	Private Key of node **b**
PK_b	Public Key of node **a**
$E_{a,b}$	Secret Key between node **a** and **b**
EK	Encryption key
$(m_{a,b})^{cek}$	Message from **a** to **b** encrypted with CEK.
t_{cek}	Time after which CEK will be changed
t_{cw}	Time after which LN and CW will be shuffled
t_E	Time after which Secret Key of all node will be revocated
$(E)^{PK_b}$	Secret Key is encrypted by PK of node **b**
LN_i	Location Number 'i' in list of CWP
CW_i	Check Word at LN 'i' in list of CWP
$CW_{i,c}$	Corresponding CW of CW_i
$(CW_{i,c})^{PK_a}$	Corresponding CW of CW_i encrypted by PK_a

Table 1: Notations

3.3 Authentication Procedure

This scheme will work in the following sequence.

- Node a will send an encrypted "identity authentication" message to all neighboring nodes which will be in its direct communication range. The message from node **a** to node **b** will be

$$(m_{a,b})^{cek} = \{ID_a, ID_b, (LN_i, CW_i)^{PK_b}\}$$

- Node **b** after receiving the message will decrypt the message using the CEK in use at that particular moment of time. Then, ID will be checked in the existing list of IDs. Thereafter, remaining message will be decrypted using $VK_{b.}$ After decryption, CW_i corresponding to LN_i will be checked. If correct, node **a** will be considered as an authentic node and will be responded by the specific reply as under

$$(m_{b,a})^{cek} = \{ID_b, ID_a, (CW_{i,c})^{PK_a}\}$$

If the message from node **a** will contain any wrong detail about ID_a , LN_i or CW_i then there will be no response to this message.

- Node **a** on getting the message from **b** will decrypt it using the CEK and will check for the ID in the existing list of IDs. Then remaining message will be decrypted using VK_a. The decrypted $CW_{i,c}$ will be than matched in the list of CWP. If found correct, node b will be considered to be an authorized node. If the message from node **b** contain any wrong detail about ID_b or $CW_{i,c}$ then there will be no response to this message. If everything proves to be correct after decryption then node **a** will send its E, encrypted by PK_b in shape of following message

$$(m_{a,b})^{cek} = \{ID_a , ID_b , (E_{a,b})^{PK_b}\}$$

- On receiving the message, node b will decrypt the message using CEK and than $VK_{b.}$ After this it will save $E_{a,b}$ sent by node a.

Any further communication between node a and b will be based on $E_{a,b}$. Step 1 to 4 will be repeated for all the nodes which are in direct communication range of node a.

3.4 Message Flow Diagram

Message flow between nodes **a** and **b** across MANET is shown in Figure 2.

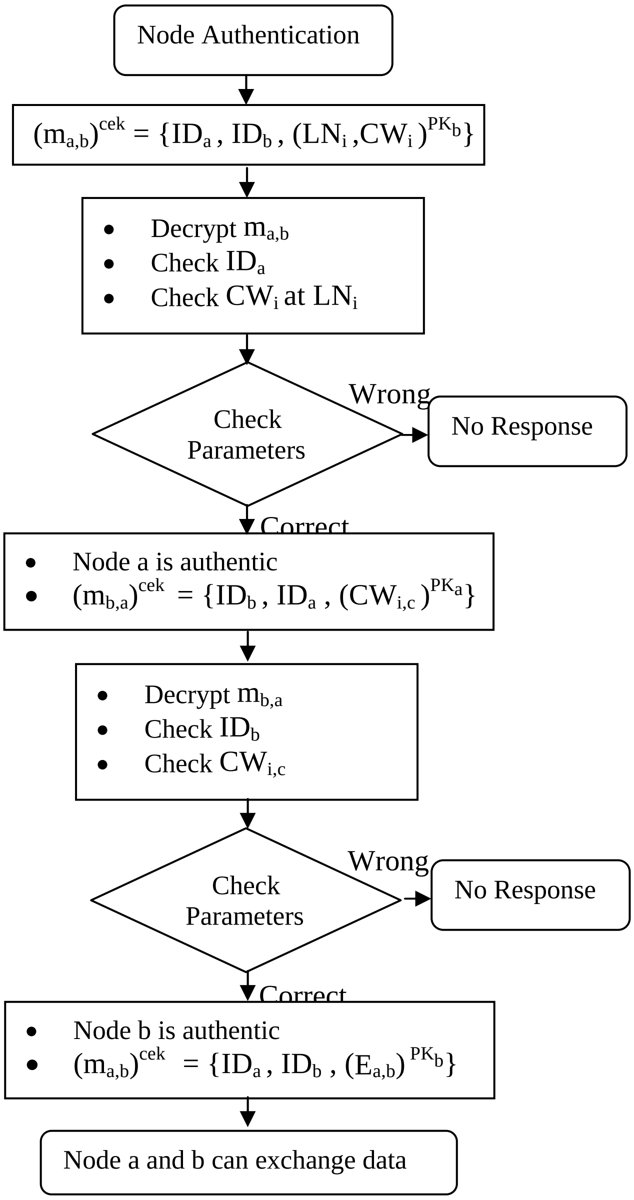


Figure 2: Message Flow

3.5 Freshness of Keys

In the above scheme, three types of encryption keys are used. Each type of key will observe the change to ensure freshness.

- Communication Encryption Key (CEK) will be used for communication encryption as the final encryption layer. As several CEKs are stored in the node so after a time interval t_{cek} the next key in the list will become the valid CEK. This will happen on all the nodes at the same time. This change will provide us with added security as it will make unauthorized access increasingly difficult.
- Check Word Pairs (CWPs) will also be changed with the time. Once the transmission of "Identity Authentication" message takes place the Location Number (LN) goes within message which if decrypted by the intruder and noted for future can create security problem. To cater for this all LNs and EKs will be shuffled after a specific time 't_{cwp}' by a specific algorithm thus making simultaneous and same type of changes on all the nodes.
- Secret Key (E) will also be changed to enhance the security of the data being transmitted. Every node will calculate, implement and transmit the E after a time interval t_E. By doing this even if a secret key is known to some unauthorized person it will be effective for a limited time period only. Once the new E for the node is issued the previous E will automatically be deleted for that node.

3.6 Incorporating New Node

If the first launch time and the current time are passed to the program, it will calculate all the changes to the CEK and CWP. Once it is done, the new node will be able to communicate with all the neighboring nodes which were already part of MANET as every node will be having its ID in the reserve list.

3.7 What if a Node is Captured?

If a node monitors that no network activity has occurred for a pre-defined span of time, it will generate a "Notify Presence" message to the neighboring nodes and if no response is received, it will consider itself to be captured and will automatically destroy all the data, keys and controlling program present on itself.

3.8 Analysis of Proposed Mechanism

Analysis of the proposed mechanism reveals following merits and demerits.

3.8.1 Merits

- The mechanism is completely capable of self organizing itself as it works in a fully distributed manner and all nodes have total independence.
- There is no requirement of any additional network infrastructure like central authority or online TTP for certificate management as all nodes are responsible for issuing, distributing and storing keys in a fully distributed manner.
- The mechanism satisfies the needs of node authentication by use of CW and key authentication by using asymmetric key cryptography for key transport. Moreover, if E is compromised, it will be of no use to the intruder, unless the format of the key is clearly known along with all the available CEK and CWP in the same sequence as are currently in use. Therefore leakage of E would not be jeopardizing the secrecy level of the network.
- All the information stored on the node is encrypted. Moreover, E on the node is in a form which cannot be easily used, so even if the node falls in the hand of unauthorized person, he will not be able to extract the information.

3.8.2 Demerits

- Each node needs extra storage space not only for the controlling program but also for storing IDs, PK, CEKs and CWPs.
- As the number of nodes in the friends list increases in the size, it will become a burden on the storage and key handling capability of a node.

4. Results

The results of node authentication mechanism are appended below.

- The communication cost of the authentication phase is directly proportional to the total number of nodes ‘N’ in the network and displacement pattern of the node based on which each node will establish communication to only the neighboring nodes ‘n’ which are in direct communication with a particular node n_i.

Communication cost c_i of the authentication phase for a node n_i is:

$$c_i = \sum_{i=1}^{n} (a + r + k).h_j$$

Where n is the number of nodes in direct communication to c_i, a and r are the message sizes of identity authentication from node i to j and identity authentication reply message from node j to i respectively, k is the message size of key carrying message from i to j and h_j is the number of hops from i to j.

To compute the communication cost of the complete network for initialization phase we use

$$C = \sum_{i=1}^{N-1} c_i - \sum_{j=1}^{k} c_j$$

Where C is the total communication cost, N is the total number of nodes in the system, c_j is the node for which c_i is already having the key, k is the number of nodes for which key is available with c_i.

5. Conclusion

In this work we have dealt with security in ad-hoc networks. We have focused on node authentication mechanism since this is the core requirement to before initiating a secure communication. We have analyzed the previous work thus highlighting the weaknesses related to node authentication. Finally, we have proposed a new node authentication mechanism which is fully distributed and has the ability to self-organize with out the requirement of any online trusted third party.

References:

[1] Bren C Mochocki and Gregory R Madey, “H-MAS: A Heterogeneous, Mobile, Ad-hoc Sensor-Network Simulation Environment”.

[2] Asad Amir Pirzada and Chris McDonald, “Kerberos Assisted Authentication in Mobile Ad-hoc Networks”, 27th Australasian Computer Science Conference, 2004.

[3] Andr´e Weimerskirch and Gilles Thonet, “A Distributed Light-Weight Authentication Model for Ad-hoc Networks”, the 4th International Conference on Information Security and Cryptology (ICISC 2001), 6-7 December 2001, Seoul, South Korea.

[4] Srdjan Cˇ apkun, Levente Buttya´n and Jean-Pierre Hubaux, “Self-Organized Public-Key Management for Mobile Ad Hoc Networks”, the work presented in this paper was supported (in part) by the National Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), a center supported by the Swiss National Science Foundation under grant number 5005-67322.

[5] Bing Wu, Jie Wu, Eduardo B. Fernandez and Spyros Magliveras, “Secure and Efficient Key Management in Mobile

Ad Hoc Networks”, Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS’05).

[6] C.E. Perkins, “Ad Hoc Networking”, Addison Wesley Professional,Dec. 2000.

[7] D.B. Johnson, “Routing in Ad Hoc Networks of Mobile Hosts,”Proc. IEEE Workshop Mobile Computing Systems and Applications,Dec. 1994.

[8] J. Jubin and J.D. Turnow, “The DARPA Packet Radio Project”,

Proc. IEEE, 1987.

[9] Srdjan Capkun, Levente Buttya´ n and Jean-Pierre Hubaux, “Self-Organized Public-Key Management for Mobile Ad Hoc Networks”, IEEE Transactions on Mobile Computing, VOL. 2, NO. 1, JANUARY-MARCH 2003.

[10] Garfinkel, S, “ *PGP:Pretty Good Privacy”*, O’Reilly& Associates, Inc., 1995.

[11] Zhou, L. and Haas, Z. J. (1999): Securing Ad Hoc Networks, *IEEE Network Magazine*, 13(6).