

## **Improving Security Features In MANET Authentication Through Scrutiny Of The Certification Revocation List Servers' Status**

B.V.Pranay Kumar<sup>1</sup>, A.Poorna Chandra Reddy<sup>2</sup>

<sup>1</sup>*Computer Science & Engineering, Christu Jyoti Institute of Technology & Science.*

<sup>2</sup>*Computer Science & Engineering, ChristuJyoti Institute of Technology & Science.*

---

**Abstract-**With changing times, the researchers find MANET Security, a daunting task. Authentication problems are cropping up frequently, in the absence of well laid out infrastructure. The adaptability of TTP's and non TTP's in MANET's becoming more difficult and impractical. With the help of pre assigned logins on offline basis and issuance of certificates more effectively can address with the help of Hybrid Key management Scheme on strength and use of 4G services. The proper account of CRL status of servers was not taken into by the scheme. If it is embedded the nodes need to check frequently the server's CRL status for authenticating any node and place external messages outside MANET which leads to overheads. To reduce them, we tried by going for online MANET authority, responsible for issuing certificates, duly considering the CRL Status of servers, their renewable and key verification within the MANET, which had sufficiently reduced the external messages.

**Keywords:** Authentication, MANET Authority, CRL, TTP, 4G, Mobile Ad hoc Network

---

### **I. INTRODUCTION**

Mobile Ad hoc Networks (MANETs) are infrastructure-less networks comprising mobile nodes and are vulnerable to attacks for lack of any specific boundary and random entry of nodes in the network. Authentication is the hallmark of security and failure to achieving this so far is a stumbling block in the way of securing MANET. At small scale the authentication can be managed by the nodes through handshaking [6], but at larger scale it becomes complex and demands the involvement of TTP [1]. Some of the schemes are either based on self-organization in MANETs without TTP [2] where the identity is resolved by nodes themselves and some are based on absolute TTP [12], while a hybrid form of these schemes can also be used [1]. Our research work is based on the optimization of a scheme known as Tseng model [1] that gets the nodes authenticated in MANET by the use of 4th generation (4G) technology [10] and [11], a future technology that supports in communicating different platforms in a transparent manner. The Tseng model allows the authentication and distribution of certificates to nodes through the support of 4G technologies. The Tseng model did not take into account the CRL status of servers. The Tseng model shows further overheads if this feature is embedded in the scheme, since, the nodes need to check frequently the server's CRL status for authenticating a node and place external messages outside MANET. If a server finds its ID in the CA's CRL directory any time it renders all the certificates of nodes invalid in the MANET. The nodes ask their servers to find the CRL status of a corresponding node's server. The communicating nodes can be from same and different CA domains. In the worst case if nodes need to establish sessions with the nodes from different servers each time, the overhead grows even more. The Tseng model, not fulfilling the requirement of CRL for the nodes to be known before authentication, can be regarded as less secure and costly for overheads when the nodes from different servers try to communicate and verify from servers with the added feature of security. We have tried to optimize the scheme by introducing an online MANET Certificate Authority in the network. A certificate is

provided to each node by MCA after testing the CRL status of each node's server. It reduces verification visits to the server frequently to a large extent for a MANET relatively larger in size and hence less overheads enhances the efficiency of the MANET. The paper is organized as follows: In section 2, an overview of previous schemes is presented. In section 3, we present the proposed model with certificate distribution and different communication scenarios. In section 4, we compare Tseng and proposed models and give simulation analysis while in section 6, we concluded our findings.

## **II. RELATED WORK**

A lot of work has been done on security problems regarding MANETS so far. We now take a brief overview of some of the related previous papers as following.

In threshold cryptographic scheme [3], the authority of CA is distributed among many  $t+1$  network nodes, called servers, to minimize the chance of a single CA being compromised. All the nodes' certificates are divided into  $n$  shares and distributed to server nodes before network formation. If a node requires other node's public key, it requests to server nodes which generate their partial signatures individually and send to combiner to form a signature and present to the asking node. In MANET it is a cumbersome process that may cost more than a MANET's formation objective.

A similar scheme [5] is an improvement over [3] on the basis of availability. Here, the CA is a fully distributed and any  $t+1$  number of nodes in MANET could behave as server nodes for issuance and verification of public keys for the nodes. Despite the advantage of availability, the scheme loses on the side of robustness with the higher values of  $t$ . The selection of  $t$  should be trade-off between both of the parameters. In KAMAN [7], multiple Kerberos servers are responsible for distributed authentication in MANET. The servers are boot-strapped with keys shared with the client nodes. The users rely upon servers for acquiring tickets after authentication to communicate with other users which is a bottleneck for its implementation in MANETS and the servers are not trusted as there is no TTP involved initially. In self-organized MANETS [2], the nodes rely on themselves for all routing, authentication and mobility management. The nodes issue certificates to their trustees for bringing them into MANET which are verified on the basis of repositories maintained by the nodes. Though, the scheme is self-organized but has the overheads of maintaining repositories which consumes the memory and bandwidth. Secondly, the originator blindly trusts any other node for making a new entry in the MANET.

A scheme [1] based on PKI implementation, resolves identity of nodes in MANET with the help of 4G services. The server distributes certificates to nodes through a special node using 4G services. The scheme successfully embeds TTP with MANET and getting nodes authenticated. However, it shows external message overheads when nodes from different servers communicate and verify the server's CRL status frequently. The scheme can be further optimized by reducing the overheads. One more scheme [12] is based on certificate distribution to nodes before network formation by a trusted third party. The drawback remains with the condition of certificate issuance by TTP before network formation to all the nodes in MANET. Some more work in this regard can be viewed in [8], [9] and [10] references.

## **III. PROPOSED MODEL**

In Tseng model [1], the overhead tends to grow with higher proportions, as more and more nodes from different servers interact and establish sessions. If the nodes communicate recurrently, they can verify one another without server by storing CRL status. In the worst case, the communication of a node with nodes of a different server for each new session leads to external

message overheads. We have tried to overcome weaknesses in Tseng model by lowering number of external messages for interacting nodes from different servers. Our scheme is based on the following assumptions.

### 3.1 ASSUMPTIONS

1. A MANET Certificate Authority (MCA) is introduced as an independent entity authenticated by CA. The MCA has both, one homogeneous card for inter-nodes communication, and other heterogeneous card for accessing the 4G services.
2. A GN is a valid user of some server in the internet that generates its own public and private key pair.
3. There is only one MCA active in the MANET at one time, which may hand the charge over to a passive MCA in MANET any time due to any reason.

abbreviations: MID: MCA ID, SID: Server ID, NID: GN ID, PKNID: Public key of GN, EPKS: Encryption through public key of Server, RNID: Random number taken by GN, PWNID: Password of GN, h: hash, Cert MCA Certificate issued by CA, SignPRM:MCA: Signature through private key of MCA, Cert: Server Certificate issued by CA, SignPRS: S Server's Signature, PKM: Public key of MCA, Cert : Certificate issued by Server1 to A, AbyS1 EV: Entity Verification, SRT: Server Restricted life Time, EP: Evaluation Point, CRL: Certificate Revocation List, TTP: Trusted Third Party

### 3.2 SYSTEM MODEL

In existing scheme [1], we have introduced an online MCA which establishes a secure channel with servers like special nodes in Tseng model. The nodes access servers on internet through MCA and the provided logins are basis of verifiable identities for getting certificates. All GNs generate their private and public keys through built-in PKI techniques. The authorities sign public keys for issuing certificates. The procedure of issuing certificates is defined in the following section.

**Certificate Issuance.** A node having a login, that wants to become part of the MANET, sends its parameters to MCA as shown in Fig. 1. MCA sends these parameters to server along with CA certificate and its signature, as shown in Fig. 2. In Fig. 3, the server verifies MCA certificate through CA's public key and the node's identity by decrypting parameters through its private key and public key of MCA. It generates hash value by taking hash on node password, decrypted random number, node's id and public key which is matched with the received hash. Then the server generates a certificate and sends along with its certificate as shown in Fig. 4. MCA generates a certificate by signing node's public key, Nounce, and expiry time for the lesser time period than the SRT.

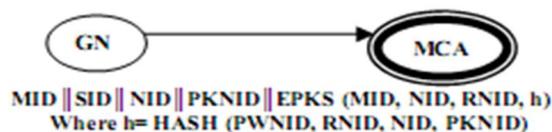


Fig. 1. Certificate Request

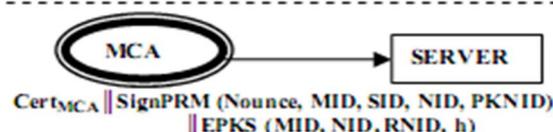


Fig. 2. Verification from Server



Fig. 3. Verification Acknowledgement

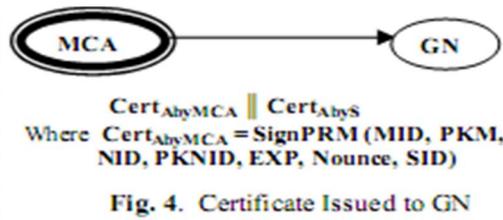
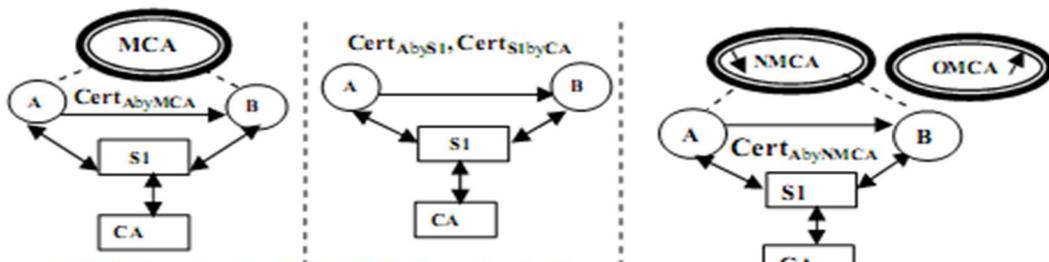


Fig. 4. Certificate Issued to GN

Whichever is lower of both server's CA issued certificate time and server's CRL time period, will be the certificate expiry time of node. A node accesses the public key of MCA through server's signed certificate which serves as a proof for MCA and GNs in authenticating one another. In Tseng model the scenario for different servers bears the overhead cost of entity verification. In proposed scheme the nodes in different servers scenario, establish sessions being under the MCA authority and the cost for finding server's CRL status and verification diminishes almost to zero as there is no external message cost for EV. The security is enhanced by taking into account the CRL status. MCA checks the CRL status of its member nodes' servers each time on certificate expiry to reissue certificates for validating authenticity. Communication Scenarios and Overheads. In the following the different communication scenarios for Tseng and proposed models are explained. New Scheme, Same Servers (NSSS) and Old Scheme, Same Servers (OSSS). In Fig. 5, part (a) and (b) the node B can verify itself the identity of A as it knows the public keys and CRL status of its server. One drawback of OSSS is removed in NSSS as CR is done within MANET as compared to CRS. In NSSS, as authentication of a node is done within the MANET like OSSS so there is not much difference in the scenarios of both models. Now, if original MCA (OMCA) moves out of the MANET, OMCA assigns a proxy certificate to a new MCA (NMCA) after verification. The GN gets a certificate from NMCA on its certificate expiry. The two nodes should be carrying the certificate from same MCA at any instant for communication.



New Scheme, Different Servers (NSDS) and Old Scheme, Different Servers (OSDS). The NSDS scenario overcomes the overhead in OSDS through MCA introduction. In OSDS, a node verifies the identity of other node by its server leading to overhead. In proposed scheme when nodes belonging to different servers come under MCA, the EV is performed by nodes within the MANET as the public key of MCA is known to all nodes. Our scheme do not incur cost for EV and overhead is reduced which leads to efficiency for the MANET as shown in Fig. 7. If OMCA moves out, the nodes switch to the NMCA as shown in Fig. 8. The nodes may regenerate certificates before the certificate expiry in case of urgent need for making contact to a node that has switched to NMCA. OMCA provides a list of node IDs to NMCA while moving out. The NMCA issues certificates to the nodes after verification of those IDs.

#### IV. COMPARISON WITH SIMULATION RESULTS

The purpose of this section is to draw the comparison of both schemes on the basis of

The NMCA issues certificates to the nodes after verification of those IDs.

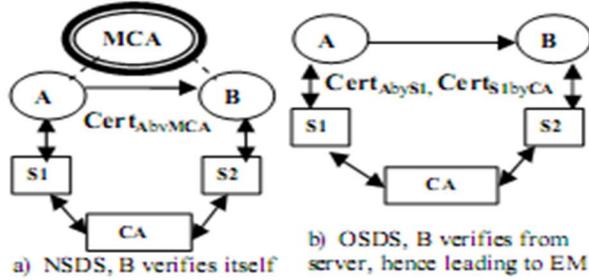


Fig. 7. Comparison of NSDS and OSDS

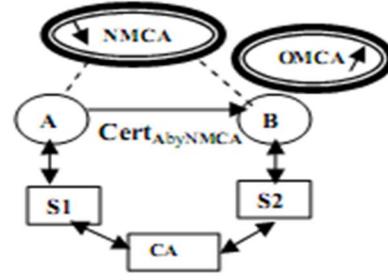


Fig. 8. NMCA replaces OMCA in NSDS

## V. CONCLUSION

In this paper, we have tried to overcome the weaknesses in Tseng model. This model does not take the CRL status of servers into account which leads to lack of security on the part of nodes and their servers. When this feature is embedded in Tseng model it shows no more optimal results and comes with external message overheads. In proposed scheme the nodes authenticate other nodes' servers within the MANET leaving the hassle of finding CRL status to an online authority, which helps saving the external messages to a large extent as evident by the simulation analysis. Secondly, the certificate renewal becomes more efficient and is performed within MANET without resorting to server. Our scheme can be regarded as the extension of previous scheme with improved features.

## REFERENCES

1. Tseng, Y. Min.: A heterogeneous-network aided public-key management scheme for MANETS. Published in Wiley InterScience, Int. J. Net. Mgmt v.17: pp.3-15 (2006)
2. Capkun, S., Buttyan, L., Hubaux, J.P.: Self-Organized Public-Key Management for Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing, V. 2, no.1, pp. 52-64 (2003)
3. Zhou, L., Haas, Z.J.: Securing Ad Hoc Networks, IEEE Net. J., v.13, no.6, pp. 24-30 (1999)
4. Brandt, I., rd, D., Landrock, P., Pedersen, T.: Zero- Knowledge Authentication Scheme with Secret Key Exchange. Journal of Cryptology (1998)
5. Kong J, Zerfos P, Luo H, Lu S, Zhang L. Providing robust and ubiquitous security support for mobile ad hoc networks. IEEE (ICNP'01), pp. 251-260 Nov. (2001)
6. Stajano, F., Anderson, R. J.: The resurrecting duckling: Security issues for ad-hoc wireless networks. In 7th Security Protocols Workshop, United Kingdom, Springer-Verlag, Berlin Germany (1999)
7. Pirzada, A., Mc Donald, C.: Kerberos Assisted Authentication in Mobile Ad-hoc Networks, the 27th Australasian computer science conference (2004)



