A New Approach to Provide Security for MANETS with 4G techniques

J.Thangakumar
Hindustan University, Chennai, India

V.Chrystal Amutha
Hindustan University, Chennai, India

.M.Roberts Masillamani
Hindustan University, Chennai, India

ABSTRACT

The security of MANET is one of the major problems for researchers and scholars. While using the Trusted Third Party and non Trusted Third Party schemes to provide communication and authentication, it results in lot of security attacks like missing packets, denial of service attacks, modify packets, Theft of nodes, error in packets etc. One of the TTP schemes addressed these issues effectively by issuing certificates on its online basis; however, the scheme suffered overheads in different communication scenarios. Another non-TTP scheme provides an authentication approach in MANETS using key management by the nodes themselves but faced the security problems due to the blind trust being put on the nodes for adding other nodes in the MANET. Both schemes results in weaknesses regarding overheads and security concerns. We are proposing a new secured Certificate Authorized Routing Protocol (CARP) to provide the secured communication in MANET. The CARP model authenticates the nodes using Fourth Generation (4G) services and enables communication after the nodes being authenticated permanently.

Keywords — CARP; Mobile Ad hoc Networks; 4th Generation Services

1. INTRODUCTION

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.
Authentication research has determined that for a positive identification, elements from at least two, and preferably all three, factors be verified. The three factors (classes) and some of elements of each factor are:

1. The ownership factors: Something the user has (e.g., wrist band, ID card, security token, software token, phone, or cell phone)

2. The knowledge factors: Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question))

3. The inherence factors: Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature, face, voice, unique bio-electric signals, or other biometric identifier).

At small scale, the identity verification can be managed by the nodes themselves, as handshaking by virtue of their proximity [5], but at relatively larger scale it becomes complex and the nodes identity verification demands the authentication involvement of TTP [1]. There are schemes that are based on the concept of self-organization in MANETS [2] thoroughly without TTP connection where the identity is resolved by the nodes themselves or some hybrid form of above two schemes might be used [1].

The 4G [11] system was originally envisioned by the Defense Advanced Research Projects Agency. The DARPA selected the distributed architecture, end-to-end Internet protocol (IP), and believed at an early stage in peer-to-peer networking in which every mobile device would be both a transceiver and a router for other devices in the network eliminating the spoke-and-hub weakness of 2G and 3G cellular systems. Since the 2.5G GPRS system, cellular systems have provided dual infrastructures: packet switched nodes for data services, and circuit switched nodes for voice calls. In 3g and 4G systems, the circuit-switched infrastructure is abandoned, and only a packet-switched network is provided. This means that traditional voice calls are replaced by IP telephony.

Cellular systems such as 4G allow seamless mobility; thus a file transfer is not interrupted in case a terminal moves from one cell (one base station coverage area)[11] to another, but handover is carried out. The terminal also keeps the same IP address while moving, meaning that a mobile server is reachable as long as it is within the coverage area of any server. In 4G systems this mobility is provided by the mobile IP protocol, part of IP version 6, and while in earlier cellular generations it was only provided by physical layer and data link layer protocols. In addition to seamless mobility, 4G provides flexible interoperability of the various kinds of existing wireless networks, such as satellite, cellular wireless, WLAN, PAN and systems for accessing fixed wireless networks.

While maintaining seamless mobility, 4G will offer very high data rates with expectations of 100 Mbit/s wireless service. The increased bandwidth and higher data transmission rates will allow 4G users the ability to utilize high definition video and the video conferencing features of mobile devices attached to a 4G network. The 4G wireless system is expected to provide a comprehensive IP solution where multimedia applications and services can be delivered to the user on an

'Anytime, Anywhere' basis with a satisfactory high data rate, premium quality and high security.
4G is described as MAGIC — Mobile multimedia, anytime anywhere, Global mobility support, integrated wireless solution, and customized personal service

An ideal MANET assumes minimal third party involvement [2] before MANET formation, but on the implementation side, the MANET with such least assumptions could be exposed to countless attacks. This sort of ideal MANET is still to be sought and till that time we will have to rely on solid TTP-based assumptions. Many schemes have been proposed so far to secure the MANET in terms of authentication, which are either insecure or require heavy computation on the side of nodes. Our research work is focused on the combination of Tseng model [1] and Capkun model [2] to reap the optimization benefits.

The Tseng model gets the nodes authenticated in MANET by the use of 4^{th} generation technology [9] and [10], 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. This model assumes two kinds of nodes in the MANET, i.e., the General nodes called as GN and the special nodes as CH. The GN possess only one adhoc network card for inter-node communication while CH having both, one adhoc network card and one heterogeneous card for communication with the server. The nodes are provided with logins and passwords on offline basis and server issues certificates online after verification of login identities. The GN gets certificate by the server through a secure channel established by the CH. The CH is also authenticated by some 4G technology like cellular network, satellite service or UAVs (Unmanned Aerial Vehicles). These services are termed as WCN-AS, wide covered heterogeneous network [1]. The cellular and satellite services have ubiquitous availability and provide a vast network coverage area for providing connectivity to the internet.

The Capkun model came up with an idea of self-organization based key management scheme. The member nodes rely on themselves for key authentication, routing and mobility management. All users, having their own public and private keys, issue certificates to their trustees for bringing them into MANET's membership. The certificates are presented to the originator of this chain who verifies the certificate on the basis of repositories maintained by the originator and the supplicator. A supplicator is one, who requests for communication or some service to the originator in the MANET. Two types of repositories are maintained by each node i.e., Updated and Non-updated repositories. Updated repositories are always kept updated by frequently exchanging certificate request and response messages. Non-updated repositories contain mostly permanent certificates that need not be updated. This maintenance of repositories demands storage capacity on the part of nodes which can be taken as a flaw.

In the Capkun model when a supplicator presents this assigned certificate to the originator along with its updated repository, the originator matches both updated repositories to find a chain till its own certificate. In case if not found, matches the non-updated repositories of both. Here if the path is found, authenticates it and rejects otherwise. The originator also checks the certificate expiry time and its user-key bindings. The certificates are periodically issued and updated before the time expires and may be revoked explicitly or implicitly. Though, the scheme is self-organized but insecure as in Capkun model the originator blindly trusts any other MANET node for making a new entry in the MANET. All the member nodes can add nodes on their will and assign certificates on behalf of their parent nodes.

We have eliminates the flaws of both models. In CARP model the nodes acquire certificates from their respective servers of different domains. The communicating nodes from different domains need to verify the identities of one another through their respective servers. In CARP scheme initially any two nodes once authenticated through external resources can issue certificates to each other in the MANET by signature of their private keys. Whenever a node is added it requires authentication from external resources from both sides. These two nodes expand the group by adding further nodes on verification and exchanging certificates. In this way a authenticated certificate is established on issuing certificates after nodes verification.

The nodes maintain repositories [2] in the same manner like Capkun model does. These repositories are used to verify the chain of certificates and validate a node belonging to the MANET. This removes the need for the node once authenticated by external resources to be authenticated again by any node belonging to the group. This saves the overhead, associated with the Tseng model, of accessing server on repeated basis for authentication of nodes already authenticated. In this way the Tseng model can be optimized by lessening the external messages overhead through reducing the verification visits to server and chains up to CA. At the same time in Capkun model the nodes bring the new nodes after verification from server into the MANET.

2. RELATED WORK

Yuh-Min Tseng proposed a cryptographic scheme [3], the authority of a private CA is partially distributed among many t+1 network nodes, called servers, to minimize the chance of a single CA for being compromised. All the nodes' certificates are divided into *n* shares and distributed to these server nodes before network formation. The server nodes generate their partial signatures individually after getting the request of public key and send to a combiner to form a single signature and present to the asking node. In a MANET it seems to be a cumbersome process to acquire any node's public key. It may cost more than the MANET's formation objective.
Zhang provides a scheme [4] is an improvement over the previous one on the basis of availability. Here, the CA is a fully distributed authority and any *t+1* number of nodes in the MANET could behave as server nodes for the issuance and verification of public keys for the nodes. While in the last scheme these server nodes were fixed and their availability chances were slightly less for being approached by the nodes. Despite the advantage of availability, the scheme looses on the side of robustness. The higher value of '*t*' brings availability but compromises robustness.
Pirzada and McDonald[6] proposed Kerberos Assisted Mobile Ad hoc Network, there are multiple Kerberos servers for distributed authentication. The nodes rely on online servers heavily for acquiring tickets and then communicate. It seems to be a serious bottleneck for implementation in MANETS. Secondly, the servers are not ensured as trusted as there is no TTP involved initially.
The Capkun [2], a self-organized scheme, blindly trusts any other MANET node for making any new entry in the MANET as mentioned above. A heterogeneous key management

scheme [1], based on asymmetric PKI technique, resolves the identity of nodes in MANET with the help of 4G services. This scheme hassuccessfully embedded the TTP with the MANET, and getting the nodes authenticated. However, the scheme shows overheads in the form of external messages to server outside the MANET when nodes belonging to different servers of other CA domains communicate. There is a room for improvement in this scheme and can be further optimized by reducing the overheads.

In key management scheme [12], a separate entity has been introduced for security enhancement and elimination of external messages. The scheme needs to be improved without introducing a separate entity in the architecture.

In scheme [11] the overlapping nodes from different symmetric key groups enables the key management without 4G external verification. However, the compromise of a single node might expose the whole symmetric group.

Some more work in this regard has been reported in references [7] [8] and [9], but with minor relevance.

3. CERTIFICATE AUTHORIZED ROUTING PROTOCOL: (CARP)

In Tseng model [1], the overhead tends to grow with higher proportions, as the nodes belonging to different CA domains interact with each for every new session. We have overcome these weaknesses in the Tseng model by lowering the number of external messages coming under communication of nodes belonging to different CA domains in the Tseng model. We have achieved this by merging authenticated certificate based Capkun model with Tseng model. Our CARP scheme is based on the same assumptions as assumed in [11]. The notations being used by the entities in the messages exchanged are given as following:

Abbreviations*:* SID: Server ID, NID: GN ID, HID: CH 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, $Cert_S$: Server Certificate issued by CA, CertNID: Certificate issued by Server to GN, SigS: Signature through private key of Server, T: Expiry time period, ChainS-CA: All chain of certificates from server up to Root CA (including intermediary CAs)

In CARP model the nodes are provided with logins and passwords through server before joining the MANET. These pre-assigned logins are the basis of verifiable identities for getting certificates. All of the nodes generate private and public keys through built-in PKI techniques. The servers sign these public keys for issuing them, certificates. A GN needs a certificate from server before joining the authenticated certificate based group. After getting certificates, the nodes with common interest form a group based on authenticated certificating approach. In CARP scheme the worst case scenario of communication among nodes from different domains has been focused, as the communication among nodes from similar domains require less overhead comparatively.

In CARP scheme, initially two nodes authenticate one another through external resources i.e. servers and then issue certificates to each other to be verified by other nodes through authenticated certificate. The nodes expand the MANET group through verification and issuing certificates to further nodes. The newly added member can verify all the members of that group through verification performed on the basis of authenticated certificate. The certificates of group members can be accessed through maintaining repositories on frequent basis, by each of the group member node.

The procedure of issuing certificates to the nodes by the server is same as in Tseng model [1] that has been explained pictorially in Fig. 1 of [11] along with exchanged parameters. We now brief the procedure of a MANET group formation.

A. MANET Groups:

The nodes having server certificates from different CA domains form a MANET group on the basis of authenticated certificate. Two nodes initially authenticate each other through their respective servers, externally. After authentication the nodes mutually issue certificates by signing the public keys of each other. The nodes can bring other nodes into MANET group membership after getting them authenticated through server. In this way a long chain of certificates leads to group formation as shown in figure 1 and 2. The nodes once authenticated from external resources and brought into group membership by any of the group member node, can be authenticated by any other member without reverting back to server for authentication. This saves the bandwidth and increases efficiency for the MANET as a whole.

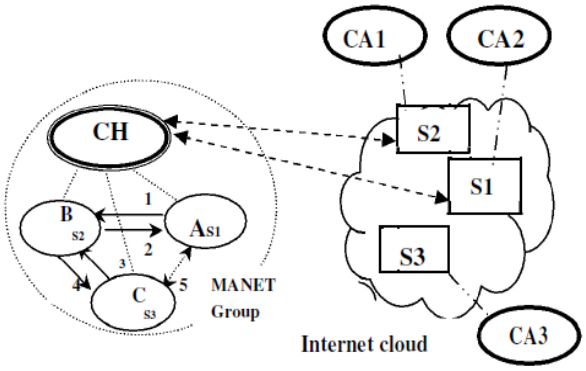

Figure. 1. The CARP Model architecture

In figure 1 the CH forwards the external messages to servers through a secure established channel using 4th generation technologies. These messages can be certificate issuance and entity verification messages. In the initial phase the nodes acquire certificates from their respective servers. In second phase the nodes of common interests form a MANET group after having verified one another through their respective servers by placing external messages to servers through CH. If the nodes belong to different servers of different CA domains as shown in figure 1, the authentication of nodes may cost very high, as being the worst case. In case all of the nodes belong to the same domain then the nodes need not making such a group as the nodes can verify the nodes from the same server by the public key of the CA known to the communicating nodes. After external and internal verification the nodes exchange their public keys or security association can be established among the entities for establishment of communicating sessions. In figure 1, a authenticated certificate has been established in the same manner. The nodes A and B authenticate and exchange certificates initially. B further authenticates C and gets it included in the group by exchanging certificates and authenticated certificate. In the same manner D, E and F are included in the group; we call them as first neighbors as these are authenticated from external resources. The nodes A and C, C and E, D and B etc, termed as second neighbors, can authenticate each other by internal verifications from certificates maintained in the repositories.

B. Communication among Group Nodes

The communicating sessions are established among the first neighbors as well as second neighbors in the MANET group after verification of nodes. The session last till the expiry time of either of the node's certificate. The certificates are expired according to the expiry of the server certificate. The first neighbors can authenticate one another without authenticated certificate verifications from the repositories. The second neighbors need to exchange repositories before establishment of communicating session. These nodes can authenticate one another by verifying the certificates of their parent nodes from the repository. If the nodes are able to find a authenticated certificate till the issuing node, the other node will be authenticated.

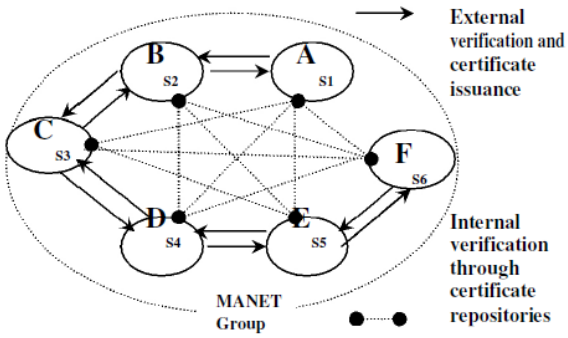

Figure. 2. MANET Certificate Authority

In figure 2, the total external messages being saved in CARP model are 20 as each side performs authentication in Tseng model. In CARP model the external verifications are eliminated when second neighbors communicate.

C.MANET dispersion

The dispersion of MANET depends upon the objective of its formation. Let suppose, one of the applications might be that some server nodes serving the client nodes on the peer level. In that case the MANET formation would be useless without the server nodes and the client nodes remain after the server nodes most of the time. The server nodes issue certificates to other server or client nodes for the time period only with respect to their own availability or interest. In this manner the MANET comes to its dispersion after the achievement of that objective automatically. The server node, just, determines the age for the MANET. There is no question of entry or exit of nodes from the MANET, as there is no specific boundary for these networks. The certificate issuance is the entry of node and its expiry being the exit.

4. COST COMPARISION

In Tseng model, external messages are required for each communicating session among the nodes belonging to different CA domains. The nodes once authenticated again require authentication on interaction with other node of the other nodes for adding a node in the MANET. There was no criterion defined in the model for identity verification of the node being added. Each node makes use of its own judgment while adding a node in the MANET which often leads to security problems. In CARP, the external messages are reduced considerably, required for verification of nodes. The second neighbors perform verification within MANET relying on low cost internal messages and certificate verifications. The communication cost of authentication in terms of external messages for 'n' number of nodes is indicated by a function, $n(n-1)$ i.e. n^2-n, for Tseng model. In CARP model this cost is minimized up to 2n-2. In Tseng model, the total cost of second neighbors for external verification amounts to n^2-3n+2, this has been excluded in the proposed CARP model

Total Cost of CARP = $n^2 - n - [n^2 - 3n + 2] = 2n - 2$

The cost in Tseng model has been measured in quadratic terms i.e n^2 which is bigoh of n^2, ($O(n^2)$), which tends to rise with increasing proportions for the increasing number of nodes. While in CARP model it is in linear terms i.e 2n and (O(n)). This indicates the difference in terms of cost for both schemes. The CARP scheme brings an aspect of security in the Capkun model by introducing external verification of nodes in the MANET. In our model the overhead tends to rise a little in comparison with Capkun model, however, we can afford this increase in cost a little for the sake of security.

5. SIMULATION RESULTS

In the simulation graph as shown in figure 3, the cost of external messages tends to rise with the increasing number of nodes and the curve has the tendency to become steep and close to the vertical axis with the increasing number of nodes in Tseng model. The curve for the CARP model lies close to the horizontal axis as the proposed model excludes the cost of authentication from external resources on the part of second neighbors' communication.

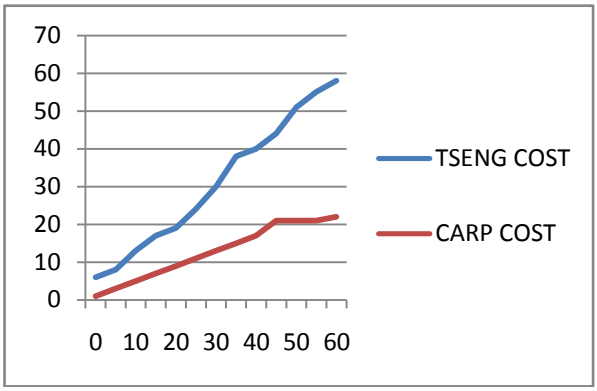

Figure 3. Reduced Carp Overhead

We have worked with the repositories based infrastructure [2] working in the background of the proposed model. The Capkun model has demonstrated the procedures for maintenance of repositories. In our scheme these repositories are used by the second neighbors for authentication of nodes leading to verification in an optimum way. Likewise, the assumptions regarding infrastructure in Tseng model are taken as pre-requisite for the proposed scheme. The nodes have no restriction for authentication from external resources; however, these nodes can avail the economies by forming a authenticated certificate based group in the MANET and authenticate the group nodes by internal verification.

6. CONCLUSION

In this CARP model, we have removed the drawbacks in two existing key management schemes by merging them in a way that the new scheme overcomes their inefficiencies regarding overheads and security. The Tseng model showed overheads on communication of nodes from different CA domains. The Capkun model was running some security problems while adding the node in MANET. The proposed scheme bears the features of both of models with eliminated defects as stated. Our proposed scheme can be regarded as an optimized extension of the existing schemes.

The nodes are issued certificates through built-in asymmetric cryptographic techniques and the sessions are

established after the verification of nodes through public keys provided by the exchanged repositories, which put off the malicious nodes to misrepresent their identities. If a node gets compromised or its private key being exposed, then its implication would last only till the certificate expiry. Thus it is recommended for the nodes to issue the certificates for a limited time period sufficient enough for logical transactions. It must be a tradeoff, as very limited time period leads to extra burden of entity verification messages and a relatively larger time period is discouraged for security concerns.

REFERENCES

[1] Yuh-Min Tseng. "A heterogeneous-network aided public- key management scheme for mobile ad hoc networks", Published on 10 February 2006 in Wiley InterScience,Int. J. Network Mgmt; 17: 3–15

[2] S. Capkun, L. Buttyan and J-P Hubaux. "Self-Organized Public-Key Management for Mobile Ad Hoc Networks ", IEEE Transactions on Mobile Computing, Vol. 2, No. 1, Jan-Mar 2003, pp. 52-64

[3]. L. Zhou, , Z. Haas, "Securing Ad Hoc Networks"

IEEE Network Journal, v.13,no.6, pp.24-30, 1999.

[4] Kong J, Zerfos P, Luo H, Lu S, Zhang L. "Providing robust and ubiquitous security support for mobile ad hoc networks", Published in IEEE ICNP, pp. 251–260, November 2001

[5]. F. Stajano and R. J. Anderson. "The resurrecting duckling: Security issues for ad-hoc wireless networks" In 7th Security Protocols Workshop, vol. 1796 of LNCS, UK, 1999. Springer-Verlag, Germany

[6]. Pirzada A., and McDonald, C., "Kerberos Assisted Authentication in Mobile Ad-hoc Networks", the 27th Australasian computer science conference, 2004

[7] Weimerskirch, A., Thonet, G., "A Distributed Light-Weight Authentication Model for Ad-hoc Networks", The 4th Intl. Conf. on Information Security and Cryptology (ICISC), 6-7, 2001

[8] Zhu, S., Xu, S., Setia, S., Jajodia, S., "Establishing pair-wise keys for secure communication in adhoc networks: a probabilistic approach", Proceedings of 11th IEEE ICNP, 2003.

9] H.Schulzrinne, X. Wu and S. Sidiroglou, "Ubiquitous Computing in Home Networks," IEEE Commun. Mag., pp. 128-135, Nov. 2003.

[10] S. Y. Hui and K. H. Yeung, "Challenges in the Migration to 4G Mobile Systems," IEEE Commun. Mag., pp. 54-59, December 2003.

[11]. A. Irshad, W. Noshairwan, M. Usman, E. Irshad, S. M. Gilani "Authentication of Nodes among Different Symmetric Key Groups in MANETs using 4G Technologies" IEEE ICCET, JAN 2009, Singapore

[12] A. Irshad, W. Noshairwan, M. Shafiq, S. Khurram, M. Usman, E. Irshad "Security Enhancement in MANET Authentication by checking the CRL Status of Servers" Springer-Verlag, SERSC-IJAST, DEC 2008, Korea