ISSN:0975-9646

Reviewing MANETs & Configurations of Certification Authority (CA) for node Authentication

Dr. Shaveta Rani[1], Dr. Paramjeet Singh[2], Raman Preet[3]

[1,2]Department of Computer Science & Engineering
P.T.U G.Z.S Campus, Bathinda, India
[3]P.G. Department of Computer Science & IT
Lyallpur Khalsa College for Women, Jalandhar, India

***Abstract*— A Mobile Ad hoc Network (MANET) is a temporary network of wireless mobile devices deployed without the aid of any pre-existing infrastructure or centralized administration. But this fascinating technology is studded with a number of serious challenges that need to be well catered before its successful deployment. These challenges include security issues related to key management, routing, node authentication, data privacy, reliability etc. In this paper we look at the node authentication issue prevailing in a MANET. In most of the proposed schemes node authentication is performed by deploying special entity called Certification Authority (CA). CA in a MANET issues certificates to every node participating in the network. A certificate signed by the CA, generally holds information comprising node's identity credential, key(s) of CA, validity period of certificate and other related certification details. Apart from issuing certificates, CA generally, verifies, alters and revokes certificates from the nodes as and when needed. A certificate is treated as a means of proving a node's identity to other participating nodes. For performing node authentication, CA is configured in a number of ways. In this paper we aim to present an overview of Mobile Ad hoc Networks (MANETs) and some configurations that are used for implementing CA , as per the existing literature.**

Keywords— M*obile ad hoc network (MANET), Authentication, Key management, Certificate Authority (CA), Cryptography, Trusted Third Party (TTP), Public key infrastructure(PKI)*

I. INTRODUCTION

A. Mobile Ad hoc Networks (MANETs)

A Mobile Ad hoc Network (MANET) is an autonomous system of mobile nodes having little or no existing network infrastructure [1][2][3][4]. These are temporary wireless networks that can be established in a spontaneous manner allowing people or organisations to work and communicate without the aid of any centralized administration or support. The participating nodes are equipped with radios which have limited propagation coverage. Due to this limitation each node can connect to a few neighbouring nodes only. If the communication link between any two nodes which are not in the same radio coverage is needed, a multi-hop radio connection is established to reach the required node(s). This is achieved by relying on other intermediate nodes to relay the required message. Thus the mobile nodes in MANETs perform dual functionality in the network- as a host and as a router. These nodes operate as routers, forwarding data packets for other mobile nodes that may be multiple hops away from each other.

B. Characteristics of MANETs

A MANET has several distinct characteristics when compared with traditional wired networks and these distinct features make its deployment and management very challenging. These characteristics are dynamic topology, constrained resources, lack of infrastructure, shared wireless medium, limited bandwidth, error prone channels and so on [5][6].

Dynamic network topology

Since the nodes are mobile, the network topology changes rapidly and unpredictably leading to varying connectivity among the nodes at different times. Nodes freely roam in the network, join or leave the network at their own will and sometimes may fail, due to any reason.

Constrained resources

The mobile nodes comprising a MANET generally possess low computational capabilities, limited battery powers and storage capacities, contributing to major limitations of MANETs.

Lack of infrastructure

There is no pre-established or well defined infrastructure to support the networking operations in a MANET, making its deployment even more difficult and challenging.

Shared wireless medium

The wireless links employed have significantly lower capacity than wired links. Moreover, the wireless medium is accessible by both legitimate nodes and attackers. Apart from this, there is evidently no clear cut boundary to separate the inside network from the outside world.

Autonomous terminals

In a MANET, each mobile terminal is an autonomous node that has to work as a host and at times as a router performing switching functions. Due to this dual functionality, usually endpoints and switches are indistinguishable in MANETs.

Distributed operation

Since the network lacks any kind of centralized control or administration, the control and management of the network is distributed among the deployed nodes. The mobile nodes involved have to collaborate amongst themselves to implement networking functions like security, routing, node authentication etc.

The remainder of this paper is organised as follows. Section II describes the applications and categories of MANETs. Security goals and tentative attack types are presented in section III. In section IV, the purpose of node authentication and functionalities of CA in node authentication are discussed. Section V presents various implementations of CA as per the existing literature. Section VI presents a summary of the issues that one needs to handle while implementing a CA. Finally this paper is concluded in section VII.

II. APPLICATIONS & TYPES

A. MANET Applications

With the increase in portable devices as well as advancements in wireless technology, ad hoc networking is gaining importance day by day with increasing number of widespread applications. This kind of networking can be applied where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to utilise. The mobility, spontaneity and ad hoc nature of these networks makes them optimal solutions for catering disaster relief communications, military rescue operations, battlefield scenarios, police exercises, urgent business events, sports events, inter vehicular communications and many more of similar nature.[5][7]

B. CATEGORIES OF MANETs

Criteria like pre-configuration, network area covered and network duration create different categories in MANETs which vary in requirements, complexity and functionality [4]. Pre-configuration criterion describes MANETS as planned and spontaneous while network area coverage divides them into local and distributive. Network duration identifies them as short term and long term MANETs [8].

Planned and spontaneous MANETs

If an ad hoc network is planned, then the participating nodes can be assumed to carry some pre-configured authentication information that would aid in resolving their identity once the network starts working. But on the other hand if the network is spontaneous then the participating nodes will not have any prior security relationships and any kind of initial setup information.

Localized area and Distributive MANETs

Based on the area spanned, MANETs are identified as Localized area and distributive MANETs. In a localized area MANET, the nodes would be in more close proximity interaction with each other (like in a classroom or conference hall) as compared to a distributive MANET where the nodes would be located some distance apart with little possibility of direct physical interaction.

Short Term and Long Term MANETs

Short Term MANETs are deployed for catering some short lived event. Participating nodes over here establish communication for a short period of time and there after may never come in contact again. These networks require speedy initialization before their deployment. Long Term MANETs on the other hand live for a longer period of time and the participating nodes need to retain secret information and trust relationships even when they leave the network.

III. SECURITY GOALS & ATTACKS

A. SECURITY GOALS IN MANETs

Security services in MANETs include the functionality that is mandatory to provide a secure networking environment comprising authentication, confidentiality, integrity, access control, non-repudiation and availability [9][10][11].

Authentication

This service is required to verify a user's identity and to assure the recipient of the message is from the source that it claims to be from.

Confidentiality

Confidentiality ensures that the data that is transmitted over the communication channel is not disclosed to any unauthorised user. Confidentiality in case of MANETs can be achieved by utilizing various data encryption techniques as in wired networks.

Integrity

This network service ensures that the data is received exactly as sent by the authorised sender and is in any case not altered during transit.

Access Control

This network service controls the access of resources such as a host system or any application in a network. To enforce this service, any user who tries to gain access to a particular resource is first and foremost identified and only after a proper verification, he is granted rights for the particular access requested for.

Non-repudiation

This network service guarantees that if a user sends a message, then he cannot deny sending that message.

Availability

The Availability service makes the network services or resources available to the legitimate users. It ensures the survivability of the established network under all circumstances.

B. SECURITY ATTACKS IN MANETs

MANETs can be quickly setup as and when needed, but, their unique characteristics pose a number of serious challenges towards their successful deployment. Mobile ad hoc networks cannot be used in practice if they are not secure. The basic characteristics of MANETs make them prone to different types of network attacks. Broadly these attacks are categorised in two major categories namely active attacks and passive attacks [8][10][11][12].

Active Attacks

These attacks are characterised by the disruption of normal network functioning. An attacker out here actively participates in either modifying the transmitted data or by introducing false information into the network. Active attacks could be internal or external. Internal attacks are from compromised nodes that were once a legitimate part of the network. Since the adversaries are already a part of the network as legitimate nodes, the attacks of this nature are difficult to detect and are more severe in nature as compared to external attacks. External attacks on the other hand are the attacks that are carried by the nodes that are not legitimate part of the network.

Passive Attacks

The greatest distinction of passive attacks is that, here the intruder or the attacker captures the transmitted data without making any modifications to it and also does not inject additional unwanted traffic to the network. The basic objective behind these attacks is to violate the confidentiality of the message. Any powerful encryption technique could be employed to safeguard against such attacks.

IV. NODE AUTHENTICATION IN MANETS

MANETs are self-organizing networks and are not dependent on pre-existing infrastructure in their operations. Furthermore, nodes in a MANET can frequently and unexpectedly join and leave the network at any instance time. This frequent node mobility leads to an ever changing topology. As in any networking technology, the acceptance and proliferation of MANET are also dependent on the incorporation of adequate security schemes in their network's design and operation. The challenge in designing MANET security schemes, in general, and node authentication schemes, in particular stems from the inability to guarantee access to any infrastructure.

To provide the required authentication, a number of schemes have been proposed. Most of the schemes are employing an entity called Certification Authority (CA) for achieving the required authentication. A CA is an entity that is trusted by all participating nodes and often provides its services in the form of certificates. A certificate is a signed statement from a CA that generally holds contents like node's identity, public key of the node, period of validity of the certificate and many more related details.

BASIC FUNCTIONS OF CA

Activities related to certification are performed by CA. CA generally issues, verifies, alters and revokes certificates from the network nodes as and when needed [8] [13].

Issue of certificates

Since in MANETs the communication has to take place between nodes that have no relationship with each other and the communication has to be established dynamically, the communicating nodes need to establish some sort of identity authentication before carrying out the required communication. A CA is deployed for this purpose. A CA registers nodes for the communication. Before issuing certificate the CA may require some unique inputs from the node so as to define its identity and then creates and issues certificates to the authenticated nodes.

Certificate Renewal

The issued certificate is valid for a specified time period, after which it must be renewed before it expires. This operation is generally done in an implicit manner and is also carried out by CA.

Certificate Revocation

Certificates can be revoked if nodes are found corrupt or compromised. A node may become compromised by an active or passive attack. A list namely certificate revocation list (CRL) is generally maintained storing the identities of all nodes that start malfunctioning or appear dangerous for the network. Also in some cases if the private key is disclosed during the valid period of certificate, the CA needs to revoke the certificate explicitly and notify the network by posting it onto the CRL to prevent its further usage.

Certificate Storage

A CA or TTP generally maintains a list of legitimate nodes and their keying details for secure communication and reference.

V. IMPLEMENTATION OF CA

The implementation of CA takes on a different format, depending on the network requirement and configuration of a particular MANET environment. Irrespective of the type of CA implementation, the objective of the node authentication should be met keeping the total cost involved in the scheme's operation as low as possible and parallelly maintaining the network's reliability. These network metrics must be met irrespective of the number of network nodes and their mobility. Two CA approaches namely centralized and distributed are mainly used for node authentication.

Centralized system for node authentication

In such a system, a CA exists centrally and is trusted by all users in the system and is often used to provide authentication from a common place. An example of this approach is the Key Distribution Centre (KDC) system. But such a centralized system is not appropriate for MANETs due to its inherent characteristics. Another popular authentication scheme namely the Public Key Infrastructure (PKI) which is recognized as one of the most accepted methods for node authentication in dynamic wired networks, is also not suitable for MANETs, since PKI also requires it's only CA to be part of the fixed infrastructure and provide its services from that fixed point. Therefore for handling node authentication in MANETs, CA should be implemented in the form of a mobile node and in that case its existence at all times cannot be guaranteed. If it becomes unavailable due to any reason, the required authentication procedure cannot be performed and the network fails to function. Also the centralised CA suffers from a single point of service denial and compromise [13] [14] [15].

Distributed system for authentication

A centralized approach for authentication is considered inappropriate for MANETs as it reduces the scalability and availability of network. Apart from this, there are chances of the centrally located CA becoming a hot spot of attacks and thereby becoming compromised.

To address these issues, it has been proposed to adopt a decentralised approach for authentication.[16]. According to the existing literature, a number of schemes have been proposed by the researchers using a distributed CA system for MANETs, in particular to improve the node authentication. In such distributed approaches, the CA's functionality is distributed to multiple nodes in the network instead of a single node. Further the implementation of such a distributed CA takes on a different format, depending on the configuration of a particular MANET environment.

A distributed CA scheme based on Randomized CAs Group (RCG) is proposed [15] in which CAs are randomly assembled in groups. All groups in the MANET are of same size with equal number of CAs in each group. Each group is a representative of a specific areas, like there could be group comprising all nodes participating from within a specific country. Further the scheme assumes that the nodes serving the functionality of CAs for aspecific group are randomly selected by the nodes in that area; e.g., nodes of a country could randomly select their CAs. If a CA node leaves the network, a new node is selected as CA by the area nodes. Every CA in this scheme carries Authentication Information (AI) that includes details like CA's public key and CRL. Every CA creates certificates for the nodes in its coverage area and signs those certificates by its private key. The issued certificates are valid for a limited duration of time and are later renewed.

Another approach based on Threshold Cryptography is employed by a number of researchers to achieve distributed functionality of CA[17]. In threshold cryptography, a pair of -public and private keys are used where the public is known by all the participating entities and its corresponding private key is divided into shares and are distributed to the entities which are later referred to as shareholders. Thus for implementing a (k,n) threshold cryptographic system, the term k is referred to as the threshold value and term n represents the number of secret shareholders. In such a system at least k out of n shareholders are required to collaborate with each other to recover the private key of the system. In any case shareholders less than k cannot recover the private key of the system.

Zhou and Hass [18], for the first time, introduced the concept of threshold secret sharing into MANETs. They proposed a partially distributed authentication scheme, based on (k,n) threshold scheme to distribute the private key of the CA to a number of randomly selected server nodes. This scheme requires k severs out of n servers to later collaborate to recover the secret key of the system. Under this scheme, an adversary has to a capture at least k nodes to crack the secret key of the system and it needs to destroy (n-k+1) share holders in order to turn off the certification service. This scheme provides security to a considerable extent under the basic assumption that k shareholders are always available for providing the authentication service. But unfortunately, the unpredictable and dynamic nature of MANETs, do not go by this assumption. At times k CA nodes may not be available, leading to the failure of their authentication service.

Kong et al.[19] proposed a totally distributed authentication scheme. Here the functionality of the CA is distributed to all the nodes in the network which in turn improves the scalability and availability of the authentication service. In their scheme, all the nodes in the network are allocated a partially encryption key and have the right to sign the system certificate. When a new node wants to join the network, it can find easily enough trustworthy nodes within its on-hop neighbourhood. This configuration of CA has both pros and cons. By improving the scalability and availability of authentication service and side by side reducing the communication overhead involved among the nodes, this scheme definitely shows an improvement over the earlier scheme. But the security provided is comparatively low. A mobile adversary just needs to capture any k nodes to crack the system secret key. Apart from this with the expansion of network it would make its maintenance and management difficult.

Capkun et al [20] proposed another authentication scheme. It is a self-organised authentication scheme based on public key chain [d]. According to this scheme each node in the networks behaves like a CA, is its own authority and has the authority to sign and verify the keys of other nodes. The certificates required for the purpose of authentication are issued and stored by the nodes themselves. For this purpose each node maintains a local certificate repository containing only few certificates that are chosen by the node according to an algorithm. However as the capacity of the certificate repository is limited, the scheme can't ensure 100% success ratio for authentication. For the sake of increasing the success ratio for authentication, each node has to store as many certificates as possible, which is not feasible in MANETs as the participating nodes generally have constrained resources in terms of storage and computational capabilities.

Yi et. al [21] proposed a scheme that deals with heterogenous networks and distributes the functionality of CA among selected nodes that are computationally more powerful and secure and also possess strong communication capabilities. But this situation might not be available all the time in all kinds of MANETs.

Gujun Wang et al. [13] have proposed yet another hybrid distributed authentication scheme for large scale MANETs. Here also the CA's functionality is distributed among multiple nodes that have strong computational and communication capabilities in the network. Here the role of CA is implemented in the initialisation phase of the network. The CA stores RSA public and secret key pair and uses its RSA secret key to sign the generated certificates for all the nodes in the network. Further Shamir's Threshold secret sharing scheme is employed to divide the RSA secret key into multiple fragments called secret key shares. The secret key shares are distributed to a subset of network nodes using threshold secret sharing technique. The chosen nodes then perform the authentication functionality of the CA in a collaborative manner.

K. Ammayappan et al. [22] have also employed a CA that is called Trusted Third Party (TTP) in the bootstrapping phase of the network. In this phase each node contacts the TTP with its unique credentials and obtains certified token for authentication purpose during the active phase of the network. TTP out here is available online and issues, revokes token and keeps the revoked tokens in CRL. It then multicasts the CRL contents periodically, to all the nodes.

In most of the schemes implementing a distributed CA functionality, the authentication operation is fulfilled by a coalition of threshold number of nodes. The participating nodes generally fulfil this task by communicating with their one hop neighbours. The number of neighbouring nodes available at a particular point of time is referred to as the node degree. But due to unpredictable node mobility, there are chances of getting a varying node degree. Times when there is a reduction in the node degree, there is a considerable increase in the certification service delay.

In schemes utilising threshold cryptography, if an adversary succeeds in compromising threshold number of nodes in the network, then it can retrieve the private key of the CA and breach the security of the system. This could happen because the threshold value chosen by the schemes is kept constant throughout the lifetime of the network [12][19].

S Raghani et al. [23] have also employed a distributed CA functionality but in a parallel course, have also taken into consideration the problems arising due to constant threshold value. Their scheme allows for a change in the threshold value and it is achieved by constantly monitoring the average node degree of the MANET deployed.

VI. Issues To Be Handled While Implementing Distributed CA

The existing literature shows the usage of centralised, partially distributed and fully distributed configurations of CA. These basic configurations are deployed in a number of varying ways to achieve the required level of security in node authentication. Irrespective of the configuration adopted, the following must be care take of :

The configuration adopted must ensure some way of ensuring the availability of CA(s) throughout the lifetime of the MANET without degrading its performance.

The certification procedure adopted must be efficient and must attempt to mitigate the breaches in the security of the MANET.

Proper mechanism must be followed to ensuring a proper node degree at all the time so that, there is not much delay in getting the authentication operation done and the network works smoothly.

Network traffic at times might be caused due to reduction in average node degree of the network. As the node degree reduces the number of requests issued by a node increase leading to a situation of increased network traffic. Under such a situation, some nodes might not be able to renew their certificates on time and become isolated. So, optimal measures must be followed to maintain controlled network traffic.

While employing threshold cryptography, the most critical parameter to be set is the threshold value. This parameter is generally chosen considering the number of participating nodes and the security requirements of the system. So, due care needs to be taken towards ensuring a proper threshold value for the MANET deployed and if required, there must be a provision to adjust the threshold value dynamically.

The scheme employed should be efficient in terms of both computation and communication. It must involve Minimal (ideally none at all) interaction among nodes

In the last but not the least, the total cost of the scheme adopted should be as low as possible and all the above mentioned issues must be handled considering the constrained resources of MANET devices.

VII.Conclusion

This paper presents the fundamentals of MANETs and discusses the varying configurations used for implementing CA as per the existing literature. The systematic analysis of MANETs and CA configurations will allow the readers to better understand these networks and node authentication in them. The contents of this paper can serve as the building block for efficient and effective node authentication schemes for MANETs.

References

[1] Jun-Zhoa Sun, “Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing”, IEEE Info-tech and Info-net, proceedings, 2001, pp.316-321.

[2] [2] C. Siva Ram Muthy, B.S. Manoj,”Ad Hoc Wireless Networks:Architecture and Protocols”,Prentice Hall PTR, May 2004, New Jersey.

[3] M. Frodigh, P. Johansson, and P. Larsson,”Wireless Ad Hoc Networking: The Art of Networking without a Network”, Ericsson Review 2000,pp. 248-263.

[4] IETF Working Group: Mobile Adhoc Networks (manet), http://www.ieft.org/html.charters/manet-charter.html.

[5] Jun-Zhoa Sun, “Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing”, IEEE Info-tech and Info-net, proceedings, 2001, pp.316-321.

[6] Baayer Aziz, Enneya Nourdine, El Koutbi Mohamed, “A Recent Survey on Key Management Schemes in MANET”, IEEE International conference on Information and Communication Technologies: From Theory to Applications (ICTTA), 2008, pg. 1-6.

[7] Dali Wei, H Anthony Chan, “Analysis of the Applications and Characteristics of Ad hoc Networks”, IEEE international conference on Communication Technology ICCT’ 06, 2006, pg. 1-4.

[8] Dawoud D.S, Richard L. Gordon, Ashraph Suliman and K Asmir Raja S.V., “Trust Establishment in Mobile Ad Hoc Networks: Key Management”, Chapter 8, available:www.intechopen.com, pp.151-192.

[9] M. Aziz and Al-Akaidi, “Security Issues in Wireless Ad hoc Networks and the Application to the Telecare project”, IEEE, 2007, pp. 491-494

[10] Rashid Sheikh, Mahakal Singh Chandel, Durgesh k. Mishra,”Security Issues in MANET: a Review”, IEEE 2010, pp. 1-4

[11] Bing Wu, Jie Wu and Mihaela Cardei, Chapter xxx –“Survey of Key Management in Mobile Ad Hoc Naetworks”, Handbook of research on wireless security, pp.1-23

[12] L.Zhou, Z.J. Haas, “Securing Ad Hoc Networks”, IEEE Network Magazine, vol. 13 (6), 1999, pp.24-30.

[13] Guojun Wang, Q. Wang, J. Cao, M. Guo,”An Effective Trust Establishment for Authentication in Mobile Ad-Hoc Networks”, IEEE 7th International Conference on Computer and Information Technology, 2007,pp. 749-754.

[14] Nitesh Saxena, Gene Tsudik, Jeong Hyun Yi, “Efficient Node Admission on Certificateless Secure communication in short-Lived MANETs”, IEEE Transactions on parallel and distributed systems, Vol. 20, No. 2, February 2009,pp. 158-169.

[15] Yong Lee and Zygmunt J. Haas, “Authentication in very large Ad Hoc Networks using Randomized Groups”, IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communication, 2005, pp. 1989-1993.

[16] Lidong Zhou and Zygmunt J. Haas, “Securing Ad hoc network” , IEEE Network Magazine, November/December 1999, pp. 24-30.

[17] A. Shamir, “How to share a secret”,Communication of the ACM, vol. 22(11). November , 1979, pp. 612-613.

[18] L. Zhou, Z.J. Hass, “Securing Ad Hoc Networks”, IEEE Network Magazine, 1998, 13(6):24-30.

[19] J. Kong, P. Zerfos, . Luo, S. Lu, L. Zang, “Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks”, Proceedings of the 9th International Conference on Network Protocols (ICNP), Riverside, California, USA, 2001.pp.251-260.

[20] S. Capkun, L. Buttyan, J. P. Hubaux, “Self-Organized Public-Key Management for Mobile Ad Hoc Networks”, IEEE Transaction on Mobile Computing, 2003, 2(1), pp.52-64.

[21] Seung. Yi and Robin Kravets, “MOCA: Mobile certificate authority for wireless ad hoc networks”, 2nd Annual PRI Research Workshop (PKI03), April 2003.

[22] Kavitha Ammayappan, V. N. Sastry, Atul Negi, “authentication and dynamic Key Management Protocol based on Certified Tokens for MANETS”, IEEE Global Mobile Congress 2009, pp. 1-6.

[23] S. Raghani, D. Toshniwal, R. Joshi, “Dynamic support for Distributed Certification Authority in Mobile Ad Hoc Networks”, IEEE International Conference on Hybrid Information Technology (ICHIT’06), 2006, pp. 424-432.