Available online at: http://www.ijmtst.com/vol3issue10.html

International Journal for Modern Trends in Science and Technology
ISSN: 2455-3778 :: Volume: 03, Issue No: 10, October 2017

Survey on Certificate Revocation in MANET

Jayanthi.E[1] | Dr. Mohammed Ali Hussain[2]

[1]Department of Computer science and Engineering, KL University, Guntur Dist., A.P., India
[2]Professor, Dept. of Electronics and Computer Engineering, KL University, Guntur Dist., A.P., India.

To Cite this Article
Jayanthi.E and Dr. Mohammed Ali Hussain, “Survey on Certificate Revocation in MANET”, *International Journal for Modern Trends in Science and Technology*, Vol. 03, Issue 10, October 2017, pp: 89-93.

ABSTRACT

Mobile Adhoc Network (MANET) is a self- configuring and infrastructure-less network which consists of mobile devices such as mobiles, laptops, PDA’s etc. Because of its lack of infrastructure, wireless mobile communication, dynamic topology, MANET is vulnerable to various security attacks. This survey paper presents an overview of developments of voting and non-voting based certificate revocation mechanisms in past few years. Certificate revocation is an important method used to secure the MANET. Certificate revocation isolates the attacker nodes from participating in network activities by revoking its certificate. Over last few years different schemes are explored for certificate revocation. In concluding section we present the limitations of the current cluster based certificate revocation scheme.

KEYWORDS: *Mobile ad hoc networks (MANETs), PKI, certificate revocation, Trust, security, threshold, CCRCV*

I. INTRODUCTION

A mobile adhoc network (MANET) consists of wireless mobile devices or “nodes”, such as laptops, cell phones, and Personal Digital Assistants (PDAs), which can move in the network system openly. Fig 1 shows the structure of MANET. In addition to mobility, mobile devices cooperate to forward packets to one another to extend the restricted transmission range of each node. This is achieved by multi- hop relaying, which is used in many applications, such as disaster relief, military operation, and emergency communication. Security is an important need for these network services. Provisioning secure communication between two nodes is main concern. Because of its characteristics, such as infrastructure-less, mobility and dynamic topology, MANET is vulnerable to various types of security attacks.

Among all security viewpoints in MANET, certificate management is generally used mechanism, which is utilized to secure applications and network services. Certification is a prerequisite to secure network communication. Certificate is a data structure in which public key is bound to the attributes by the digital signature of the issuer, and can be used to verify the identity of individual, and also to prevent tampering and forging in mobile ad hoc networks.

Need for Certificate Revocation: Certificate management is basically used to covey trust in public key infrastructure to secure network services and applications.

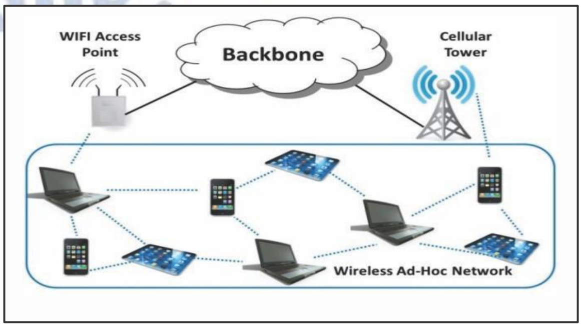

Fig 1: Mobile Ad hoc Network

The general ad hoc network characteristics are:

Mobility: Rapid deployment in areas with no infrastructure often implies that the users must explore an area and perhaps form teams/swarms that in turn coordinate among themselves to create a taskforce or a mission. We can have individual random mobility as our base mobility pattern. The mobility can have major impact on the selection of a routing scheme and can thus influence performance.

Multi-hopping: a multiple hop network is a network where the path from source to destination traverses several othernodes. Ad hoc often exhibit multiple hops for congestion control, spectrum reuse, and energy conservation.

Self-organization: The ad hoc network must autonomously determine its own configuration parameters including: addressing, routing, clustering, position identification, power control, etc.

Energy conservation: most ad hoc nodes have limited power supply and no capability to generate their own power. Energy efficient protocol design is critical for longevity of the network.

Scalability: In some applications the ad hoc network can grow to several thousand nodes. Hierarchical construction, Mobile IP or local handoff techniques do dilute the issue but still large scale is one of the most critical challenges in ad hoc design.

Security: The challenges of wireless security are well known ability of the intruders to eavesdrop and jam/spoof the channel. Ad hoc networks are more vulnerable to attacks than the infrastructure counterparts. Both passive and active attacks are possible.

Purpose of the Study Review:

The main purpose of this literature survey is to take review of the existing work in this area to understand the depth of

certificate revocation in mobile ad hoc network. Here

presents study of the existing work which makes understand the adhoc networks, issues related to mobile nodes issues related to certificate revocation, application of ad hoc networks.

Vulnerabilities of MANET:

1. Unreliability of wireless links between nodes:

Because of the limited energy supply and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.

2. Dynamic topologies:

Nodes are free to move randomly; thus, the network topology which is typically multi-hop may changes frequently at any time.

3. Lack of Secure Boundaries:

There is not such a clear secure boundary in the mobile ad hoc network, which can be compared with the clear line of defense in the traditional wired network. This vulnerability originates from the nature of the mobile ad hoc network, because of this MANET is prone to various security attacks.

4. Threats from Compromised nodes Inside the Network: Because of the mobility of the ad hoc network, compromised node can frequently change its attack target. and perform malicious behavior to different node in the network, thus it is very difficult to track the malicious behavior performed by a compromised node especially in a large scale ad hoc network.

5. Lack of Centralized Management Facility:

Due to absence of centralized management facility problems detection of attacks, path breakages, transmission impairments and packet dropping, breakage of the cooperative algorithm take place because decision making process is decentralized.

6. Restricted Power Supply:

The problem that may be caused by the restricted power supply is denial-of-service attacks.

7. Active and Passive attacks:

• Active Attack:

An active attack disrupts the normal functioning of the network by modifying or destroying the data being exchanged. It is internal and external. Internal attack can be possible by compromised node.

External attacks are conducted by the nodes which are not belongs to the network.

• Passive Attack:

Passive attack does not affect the normal operation of the network. The attacker observes the data exchanged in the network without modifying it.

II. . LITERATURE SURVEY

It is difficult to secure MANET, because of the vulnerabilities of wireless links, the limited protection of nodes, the dynamically changing topology and the lack of infrastructure. Various certificate revocation techniques have been proposed in literature to improve the network security. These revocation techniques are basically categories in voting based and non-voting based schemes.

Voting based mechanism: Voting based mechanism is characterized as the method for revoking a malicious attacker's certificate through votes from legitimate neighboring nodes.

A. Ubiquitious and Robust Access Control for MANET

The strategy proposed in [2] considers the issue of access control for a mobile adhoc network. With the help of this we give access to well carrying on nodes and deny access from acting mischievously nodes. A mischievously acting node can be either a selfish nodes or malicious node. Proposed URSA fully localized design paradigm to provide ubiquitous and robust access control for MANET. This arrangement takes ticket-based methodology. Every well-behaving node uses a certified ticket to take part in routing and packet forwarding. Nodes without legitimate tickets are classified as being misbehaving node. They will be denied from any system access, despite the fact that they move to different areas. In URSA, different nodes in a local network neighborhood, typically one or two-hop away, cooperate to monitor a node's behavior and determine whether it is well-behaving or misbehaving by using certain detection mechanism. The expiring ticket of a well-behaving node will be renewed collectively by these nearby observing neighbors, while a misbehaving node will be revoked of its ticket. The implementation is based on refined threshold cryptography algorithms. When a number of negative votes exceed a predetermined number, the certificate of accused node will be revoked.

B. Localized Certificate revocation scheme

In [4] introduces localized certificate revocation scheme. This scheme manages the issue of certificate revocation in MANET, where online access to (CA) Certificate Authority is a challenging problem. This method is used in pure ad hoc networks, where no access to central authorities or certificate authority. This solution is a decentralized certificate revocation scheme that allows the nodes in MANET to revoke the certificate of malicious entities. In this scheme each node monitors the behavior of the other nodes. If node found that given node is behaving suspiciously, it is required to broadcast an accusation packet against that node. Accusations from any given node are weighted based on trust of the accuser: the higher the trust of a node, the greater the weight of its accusations, and vice versa. A nodes certificate is revoked if the estimation of the total of accusation weights against the given node is greater than a threshold. Since all the nodes are required to participate in each voting, communication overhead is very high.

Non-voting based mechanism: In this mechanism any node with legitimate certificate can choose given node as malicious attacker.

C. Suicide for the Common Good:Credential revocation scheme for MANET

In [3] proposed scheme considered the problem of credential revocation in self-organizing systems. This is decentralized system, where certificate revocation can be immediately finished by only one accusation. However the certificates of the both accuser and accused node have to be revoked simultaneously. Therefore the accusing node has to sacrifice itself to remove an attacker from the network. This method reduces the revocation time and communication overhead of certificate revocation. The suicidal approach does not take into account the false accusation from malicious attacker. Trouble with this approach is that a malicious node can falsely accuse legitimate nodes. Therefore the accuracy of the system is degraded.

D. Certificate Revocation to cope with false accusation

In [5] proposed certificate revocation to cope with false accusation. It solves the problem of false accusation, where malicious attacker node accused the legitimate node. In this scheme, CA is responsible to handle all control messages and holding accuser and accused node in warning list (WL) and black list (BL). It is cluster based solution, Cluster head (CH) detect falsely accused node and remove from black list. In the proposed scheme, a genuine node can be recorded in the BL by a false attack detection packet sent from a malicious node. To adapt with this issue, CHs are permitted to carry out the certificate recovery to correct the mistakes in the BL. This scheme takes very short time revoke certificate of malicious attacker. Nirwan Ansari [1] proposed cluster based revocation scheme CCRVC (Cluster-based certificate revocation with vindication capability for MANET). Here nodes are organized to form clusters. In this scheme certificate authority CA manages the warn list and black lists and issues and remove the certificate of malicious nodes. If any node behaves maliciously then its neighbor node will accuse it to CA and that node placed in black list. Then CA will send accusations to CH to confirm that nodes in the black list are malicious attacker or not. If CH found that attacker then its certificate of malicious nodes are revoked. Otherwise the nodes are recovered from warning list. This scheme solves the problem of false accusation and reduces the revocation time as compared to voting based mechanism. The main limitation of this approach is very high communication overhead.

E.Certificate Revocation system based on Trust mechanism:

The system proposed in [14] is divided into three phases:

- Cluster Formation Phase
- Trust Calculation Phase
- Enhanced Certificate Revocation Phase

During cluster formation groups of mobile nodes are formed using weighted clustering algorithm. Next trust calculation phase, in which trust on each node is computed. Trust in a network is used to determine the relationship between nodes. Trust is based on its previous behavior in forwarding and dropping packets during transmission. Each and every nodes observes their nearby nodes whether it forward/drops the packets.The trust vector is modified for each transaction. So, the Enhanced Certificate Revocation algorithm is used to revoke the certificate of malicious nodes. ECR achieves the following:

- It examines the exact malicious node without any fake accusation in the cluster with two levels of accusation process.
- Proposed scheme requires AP (accusation packet) transferred across the accuser, CH and CA, which is sufficient to detect the improper nodes and thus, it reduces communication complexity.

It minimizes the period of revocation

III. COMPARITIVE STUDY

Aim of this survey is to compare various certificate revocation methods and to know their limitations. Thispaper explains the fundamentals of certificate revocation process. Then the concept of voting based and non-voting based certificate revocation has been discussed at length in this paper. From this study it has been observed that previous certificate revocation scheme has issues like processing overhead and messaging overhead. Table1. shows the comparative analysis of certificate revocation schemes

TABLEI.COMPARITIVESTUDY

Certificate Revocation Scheme	**Advantages**	**Limitations**
URSA-Ubiquitous andRobust Access Control	•Certificaterevoke basedonvotesfrom its neighbor. •Whennegative votesexceedsome	•Determining thresholdis challenging. •Doesnotdeal with falseaccusation.
Localized Certificate revocation scheme[4].	•AswithURSA,no CAexists. •Revocationis basedonweighted accusation. •Certificaterevoked whenweightedsum	•Sinceallnodes Participatein voting, highcommunication overhead. •Increasesrevocation time.
Suicidefor Common Good:New strategyfor credential revocation [3].	•Revocationquickly Completedby only oneaccusation . •Accusingnodehas to sacrificeitself.	•Doesn’tdeal with Falseaccusednode. •Accuracydegraded.
CCRVC (Cluster based Certificate Revocation with Vindication Capability for MANET)[1].	•Clusterbased Scheme. •CAmanagesWLand dBL. •Certificateof maliciousnodecan be revokedby single neighbor. •Dealswithfalse accusation.	•High Communicatin overhead.

The above studied systems are voting based and non-voting based certificate revocation in the literature survey are giving good results but they are carrying few disadvantages with them like for voting based scheme processing and communication overhead during revocation. It is also challenging task to calculating threshold in voting based scheme. From previous solutions it has been seen that, accurate revocation, quick revocation, also small network overhead remain the challenging issues to be addressed in a certificate system, particularly in MANET. The Enhanced Certificate Revocation system is designed to provide efficient certificate revocation that overcomes the drawbacks of previous schemes.

IV. Conclusion

The aim of this survey is to compare various certificate revocation methods and to know their limitations. This paper explains the fundamentals of certificate revocation process.Then the concept of voting based and non-voting basedcertificate revocation has been discussed at length in this paper. From this study it has been observed that previous certificate revocation scheme has issues like processing overhead and messaging overhead. From previous solutions it has been seen that, accurate revocation, quick revocation, and small network overhead remain the challenging issues to be addressed in a certificate system, particularly in MANET

References

[1] W. Liu, H. Nishiyama, N. Ansari, and N. Kato, ”Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks”, IEEE Trans. On parallel and distributed systems, vol. 24, no2, February 2013.

[2] H. Luo , J. Kong, P. Zerfos, S. Lu, and L. Zhang, “URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks,” IEEE/ACM Trans. Networking, vol. 12, no. 6, pp.1049-1063, Oct. 2004.

[3] J. Clulow and T. Moore, “Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems,” ACMSIGOPS Operating Systems Rev., vol. 40, no. 3, pp. 18-21, July 2006.

[4] G. Arboit, C. Crepeau, C.R. Davis, and M. Maheswaran, “A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks,” Ad Hoc Network, vol. 6, no. 1, pp. 17-31, Jan. 2008.

[5] K. Park, H. Nishiyama, N. Ansari, and N. Kato, “Certificate Revocation to Cope with False Accusations in Mobile Ad HocNetworks,” Proc. IEEE 71st Vehicular Technology Conf. (VTC’10), May 16-19, 2010.

[6] W. Liu, H. Nishiyama, N. Ansari, and N. Kato, “A Study onCertificate Revocation in Mobile Ad Hoc Network,” Proc. IEEE Int’l Conf. Comm. (ICC), June 2011.

[7] Zaiba Ishrat, “Security issues, challenges & solution inMANET”, IJCST Vol. 2, Issue 4, Oct . - Dec. 2011.[8] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in Mobile Ad Hoc Networks: Challenges and Solutions,” IEEE Wireless Comm., vol. 11, no. 1, pp. 38-47, Feb. 2004.

[8] L. Zhou and Z.J. Haas, “Securing Ad Hoc Networks,” IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Nov./Dec.1999.

[9] B. Kannhavong, H. Nakayama, A. Jamalipour, Y. Nemoto, and N. Kato, “A Survey of Routing Attacks in MANET,” IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007.

[10] Dipti S. Sawant, E. Jayanthi, “Cluster-based Certificate Revocation in mobile Ad hoc network using Fuzzy Logic”, IJCEA, 2321-3469 , Volume 9, Issue 7, July 2015.

[11] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in Mobile Ad Hoc Networks: Challenges and Solutions,” IEEE Wireless Comm., vol. 11, no. 1, pp. 38-47, Feb. 2004.

[12] L. Zhou and Z.J. Haas, “Securing Ad Hoc Networks,” IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Nov./Dec.1999.

[13] SJ. Indhu Lekha, R. Kathiroli, “Trust Based Certificate Revocation of Malicious N odes in MANET.”,(ICACCCT), IEEE International Conference on Advanced Communication Control and Computing Technologies,2014.

[14] A.Rajaram, Dr. S. Palaniswami, “Detecting Malicious Node in MANET Using Trust Based Cross-Layer Security Protocol. ”,(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (2),130-137,2010.

[15] Kannan Govindan, Prasant Mohapatra, “Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey. ”,International Journal of Innovative Research in Computer and Communication Engineering, Communications Surveys Tutorials, IEEE (Volume:14 , Issue: 2)-2012.