International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-6, August 2014

Certification Revocation in Cluster Based MANET using Rerouting Mechanism

Pradnya N. Shinde, M. S. Chaudhari

Abstract- MOBILE ad hoc networks (MANETs) now a days acquires attention of researcher, investors and manufactures due to their mobile nature , easy positioning and hot pluggable nature of involving devices into network . However, the wireless natures reduces security hence MANET becomes more defenseless to various types of security attacks than the cable connected networks. To overcome this challenge various approaches came forward. Cluster based Certificate Revocation with Vindication Capability (CCRVC) is one of them. This approach successfully overcome security challenge but did not pay attention on congestion in network as well as it has no solution for node failure. Proposed system improves CCRVC approach by applying label switched path algorithm which overcome problem of congestion and also gives solution for node failure also.

Index Terms—About four key words or phrases in alphabetical order, separated by commas.

I. INTRODUCTION

MOBILE ad hoc networks (MANETs) are widely used in recent years. Due to mobility feature, dynamic topology and ease of deployment MANETs become very popular. A mobile ad hoc network is a self-controlled wireless network which consists of mobile devices, such as laptops, cell phones, and Personal Digital Assistants (PDAs). These devices can move freely in network. Mobile devices cooperate and forward packets for each other to extend the limited wireless transmission range of each node. MANETs are used for various applications like disaster relief, military operation, and emergency communications. Because of the vulnerability of these networks security is the important requirement for these network services. Providing protected communications between mobile nodes in a hostile environment, in which a malicious attacker can launch attacks to break network security, is a primary concern. As the absence of infrastructure, mobile nodes in a MANET act as both end users and routers which relay packets for other nodes. MANET is the open network where nodes can join and leave the network freely. Therefore, the wireless and dynamic nature of MANET makes it more vulnerable to various types of security attacks than the wired networks. Among all security issues in MANETs, certificate management is a widely used technic to secure applications and network services. Certification is a primary requirement to secure network communications. It is defined as a data structure in which the public key is bound to an attribute by the digital signature of the issuer, and can be used to verify that a public key belongs to an individual node and to prevent tampering and forging in mobile ad hoc networks.

Manuscript published on 30 August 2014.
***** Correspondence Author (s)
Ms. Pradnya N. Shinde, Department of Computer Engineering, Sinhagad Institute of Technology, University of Pune, India.
Mr. M. S. Chaudhari, Department of Computer Engineering, Sinhagad Institute of Technology, University of Pune, India.

Many research efforts have been dedicated to prevent malicious attacks on the network. Any attack should be identified as soon as possible. Certificate revocation a technic of enlisting and removing the certificates of nodes that have been detected to launch attacks on the neighborhood, i.e. if a node is compromised or misbehaved, it should be removed from the network and cut off from all its activities immediately Some existing approaches such as voting based mechanism and non-voting based mechanism can quickly identifies malicious node. These mechanisms revokes malicious attacker´s certificate through votes from valid neighboring nodes. But these approaches could not pay attention on false accusation by attacker node. Cluster based Certificate Revocation with Vindication Capability (CCRVC) overcome this approach by providing certificate based approach. This approach have saviour problem of generating excess data packets in network which leads to congestion problem. Hence we propose a system which makes use of label switched path helps in congestion control, produced by flood packets in network.

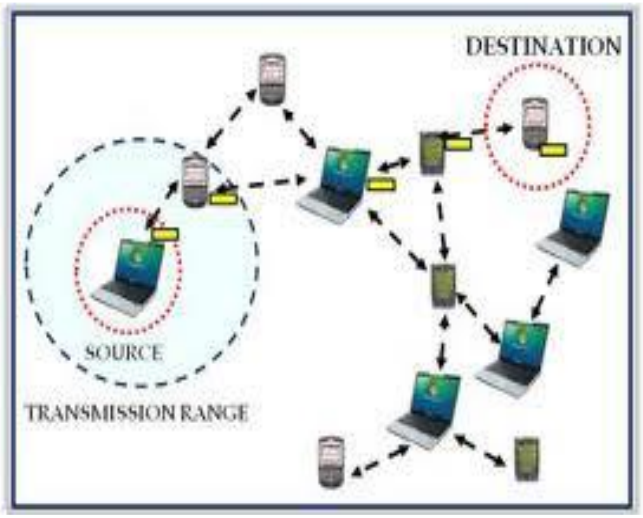

Fig. 1 Mobile Ad Hoc Network

II. PROCEDURE FOR PAPER SUBMISSION

Some existing approaches for certificate revocation, which are classified into two categories: voting based mechanism and non-voting based mechanism. [1][2][5][4]. Voting Based Mechanism This mechanism is defined as the revoking a malicious attackers certificate through votes from valid neighbouring nodes. The certificates of newly joining nodes are issued by their neighbours. The certificate of an attacker is revoked on the basis of number of votes from its neighbours.

In URSA, each node performs one hop monitoring, and exchanges monitoring information with its neighbouring nodes. When the number of negative votes exceeds a predefined number, the certificate of the accused node will be revoked. Since nodes cannot communicate with each other without valid certificates, revoking the certificate of a voted node implies isolation of that node from network. Determining the threshold, however, remains a challenge. The certificate of an accused node is revoked when the sum of votes against the node exceeds a predefined threshold. However, since all nodes are required to participate in each voting, the communications overhead used to exchange voting information is quite high, and it increases the revocation time as well. Non-Voting Based Mechanism In the non-voting based mechanism, the malicious attacker node will be decided by any node with a valid certificate. [16] proposed a fully distributed suicide for the common good strategy. In this strategy certificates of both the accused node and accusing node have to be revoked simultaneously. [3] proposed a cluster based certificate revocation mechanism, where nodes are self-organized to form clusters. In this mechanism, a trusted certification authority is responsible to manage control messages, holding the accuser and accused node in the warning list (WL) and blacklist (BL), respectively. The certificate of the malicious attacker node can be revoked by any neighbouring node. The cluster based revocation scheme, which can quickly revoke attacker node upon receiving only one accusation from a neighbouring node. The scheme maintains two different lists, warning list and blacklist, in order to protect against malicious nodes from further framing other true nodes. The cluster head (CH) can address false accusation to recover the falsely revoked nodes. Due to addressing only the issue of certificate revocation, not certificate distribution, the scheme assumes that all nodes have already received certificates before joining the network. Instead, we focus on the procedure of certificate revocation once a malicious attacker has been identified, instead of the attack detection mechanism itself. Each node is able to detect its neighbouring attacker nodes which are within one hop away. It can also handle the issue of false accusation that enables the falsely accused node to be removed from the blacklist by its cluster head (CH). It takes a short time to complete the process of handling the certificate revocation. Since the blacklisted nodes cannot take part in network activities, restoration of traffic is required. The restoration can be performed by rerouting of packets using Label Switched Path (LSP). Node blacklisting causes link failure. There are two basic methods for LSP recovery:[4] (1) Dynamic rerouting and (2) Fast rerouting [4]. Fast rerouting uses pre-established alternative LSPs or LSP segments. Disadvantages of Existing Systems

Voting Based Mechanism:

Disadvantage: Since all nodes are required to participate in each voting, the communications overhead used to exchange voting information is quite high, and it increases the revocation time as well.

Non-Voting Based Mechanism:

Disadvantages: Degraded accuracy in determining an accused node as malicious node, degraded reliability of certificate revocation.

Label switch [3] In case of hop by hop router configuration, packets enter into the router, after that router read the packet header, and then the router sends the packet to the next hop according to the destination address. But label switched network is having different working style; Packets will not be forwarded on a hop by hop basis. Instead, paths are previously determined for particular source to destination pairs. MPLS network topology. In the topology of an IP routed network [2], traffic from router 1 is forwarded to router 4, which then makes its own forwarding decision, and so on, until the packets arrive at router 9. In a label switched network, a route from router 1 to router 9 is created so that all traffic from router 1 to router 9 takes the same deterministic route. Because a route already exists, individual routing nodes don't need to do a forwarding lookup on the packets as they enter the router. Instead, each node must keep information on the paths that have been already established through it (so switching tables tend to be much smaller than routing tables). As packets from that flow enter a router, the router can switch the packets on to a predefined path toward its destination through the network. Put simply, if router 4 knows that for all traffic from router 1 to router 9, the next stop along the way is router 6, it can just forward the packets to that predetermined hop without ever looking up the route in its routing table.

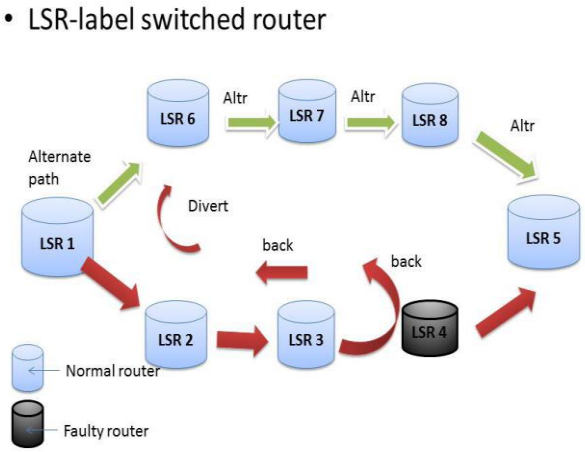

Fig. 2 Label Switched Network

Label Switched Paths:

The pre-set paths that make MPLS work are called label switched paths (LSPs). Routers in an MPLS network exchange MPLS information to set up these paths for various source destination pairs. Important thing over here is that every router along the LSP from router 1 to router 9 must have the same view of the LSP. If a switched path is to have real efficiencies over typical IP routing, every router on the LSP must be able to switch the packet forward. MPLS is often called a layer 2.5 technology because it shares both routing (layer 3) and switching (layer 2) characteristics. The fact that paths are pre-set makes MPLS behave quite like a layer 2 protocols. However, capability of MPLS to use signalling protocols, which themselves relies on routing knowledge for LSP establishment and traffic engineering and adjusts on the fly.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

III. IMPLEMENTATION DETAILS

A. *Algorithmic Steps*

Implementation of AODV, Certificate Revocation Algorithm and Minimizing False Accusation Algorithm.

Deriving and calculating optimum threshold value.

Proposed system:

1. Firstly Ingress LSR (Label Switched Router / Source) sends data packets on a protected LSP (Label Switched Path) i.e. the normal path which it is using to send the packets to the specified Outgress LSR (Destination).

2. The intermediate LSRs maintain a local buffer where they store a copy of the ongoing packets.

3. Once the FAULTY LSR is detected the flow of data packets stops there itself.

4. Then the Swapping operation is performed between the Faulty LSR and the Backward LSR i.e. the previous LSR.

5. Swapping operation is basically the swapping of tags which would be used to maintain the order of the packets, i.e. the order of the packets in which they were being sent to the Outgress LSR will be restored.

6. Now Data Backtracking process will begin from the Faulty LSR back to the Ingress LSR, so that Ingress LSR can send the packets in the preserved order of packets.

7. Every LSR maintains their link status in LIB (Local Information Base table) in the form of input label, output interface.

8. When the Faulty LSR redirects the data packets in the reverse direction of the protected LSP the link status of that particular LSR changes from NORMAL to FAULT DETECT.

9. After performing Swapping operation, the backward LSR which receives the data packet from the FAULTY LSR changes its link status in its respective LIB to ALTERNATIVE DETECT, which indicates that there is some problem in the protected LSP.

10. Now as the data packet is sent back to backward LSRs, the LSRs will update their local buffer with the current data packets being received and accordingly they will update their link status in their respective LIBs from ALTERNATIVE DETECT to STORE BUFFER and the process continues till the tagged packet is received from backwards packet.

11. Now in order to check the order of the tagged packets the LSRs has to check the tag bit of the received packets from backwards LSP is set(1) or not i.e. (0). If the comparison result is false the packet will be forwarded using normal swapping operation. Otherwise, it knows that no more packets are expected from backwards LSP.

B. *Mathematical Model*

C. *Data Flow Diagram*

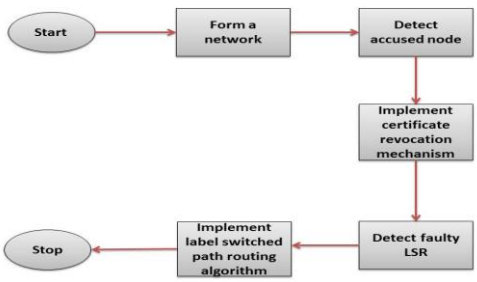

Fig. 3 Data Flow Diagram

IV. RESULT AND DISCUSSION

Among all security issues in MANETs, certificate management is a widely used mechanism which serves as a means of conveying trust in a public key infrastructure to secure applications and network services. A complete security solution for certificate management should encompass three components: prevention, detection, and revocation. Certificate revocation is an important task of enlisting and removing the certificates of nodes who have been detected to launch attacks on the neighbourhood. Hence Cluster based Certificate Revocation with Vindication Capability (CCRVC) scheme which is our proposed scheme overcomes all the loop holes and disadvantages of the existing techniques and mechanisms.

1. Correct Input

In most recent known inputs, users enter correct input and is done with polynomial time i.e. it comes under P type. User is giving requirement in NP complete form; if input is not in proper format the operation fails, so we always give proper input, by doing so we will reduce redundancy which increases efficiency of the system.

2. Wrong Source or Destination or Null message

It happens when user gives wrong input, in that case he cannot complete the work in polynomial time, and hence it falls in NP hard type. In our project we are providing Correct your input field facility, with the help of which user can correct the input and execute it. Hence it comes under P type, which then comes under NP complete.

V. CONCLUSION

In our proposed system we are proposing a Cluster based Certificate Revocation with Vindication Capability (CCRVC) scheme, where the cluster head plays an important role in detecting the falsely accused nodes within its cluster and recovering their certificates to solve the issue of false accusation. On the other hand, CCRVC inherits the merits of both the voting based and non-voting based schemes, in achieving prompt revocation and lowering overhead as compared to the voting based scheme, improving the reliability and accuracy as compared to the non-voting based scheme. Our scheme can quickly revoke the certificate malicious device, stop the device access to the network, and enhance network security.

Summary of advantages of proposed system

1. Prompt Revocation of malicious nodes.
2. Reduced Communication overhead as compared to Voting based mechanism.
3. Improved Accuracy as compared to Nonvoting Based Mechanism.
4. Improved reliability of certificate revocation.
5. Enhance network security by quickly removing the certificate of malicious node thereby removing it from network.

VI. ACKNOWLEDGMENT

I take this opportunity to extend my deep sense of gratitude and words of appreciation towards those who helped me during the pursuit of my present study.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

It gives me great pleasure and satisfaction to express my deep sense of gratitude towards my Post Graduate Guide Prof .M.S.Chaudhari for accepting me as his student and gave me immense support during this Seminar work from beginning to end, in spite of his very busy schedule. I feel extremely fortunate to have him as my guide. My sincere thanks to Mr. Chaudari Sir P. G. coordinator, Prof. T. J. Parvat HOD CE Dept., Dr.M.S.Gaikwad Principal, SIT,Lonavala.

REFERENCES

[1] R. Callon, P. Doolan, N. Feldman, A. Fredette, G. Swallow, and A. Viswanathan, A framework for multiprotocol label switching, Internet draft¡draft-ietfmpls- framework-05.txt¿, September 1999.
[2] E. Rosen, A. Viswanathan, and R. Callon, Multiprotocol label switching architecture , RFC 3031,, January 2001.
[3] D. Awduche, J. Malcolm, J. Agogbua, M. O Dell, and J. McManus, Requirements for traffic engineering over mpls , RFC 2702, September 1999.
[4] V. Sharma, Ben-Mack Crane, S. Makam, K. Owens, C. Huang, F. Hellstrand, J. Weil, L. Andersson, B. Jamoussi, B. Cain, S. Civanlar, andA. Chiu, Framework for mpls-based recovery, Internet draft¡draftietf- mpls-recovery-frmwrk-01.txt¿,, November 2000.
[5] D. Haskin and R. Krishnan, A method for setting an alternative label switched paths to handle fast reroute, Internet draft¡draft-haskin-mplsfast- reroute-05.txt¿, November 2000.
[6] S.Makam, V.Sharma, K.Owens, and C.Huang, Protection/restoration of mpls networks, Internet draft¡draft-makam-mpls-protection-00.txt¿, October, 1999.
[7] G. Swallow, Mpls advantages for traffic engineering, in IEEE Comunication Magazine, pp 54-57, December 1999.
[8] L. Andersson, P. Doolan, N. Feldman, A. Fredette, and B. Thoma,Ldp specification,, RFC 3036,, January 2001.
[9] Daniel O. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, and G. Swallow,Rsvp-te: Extensions to rsvp for lsp tunnels, draft ¡draftietf-mpls-rsvp-lsptunnel- 07.txt¿, August 2000.
[10] E. Rosen, D. Tappan, G. Fedorkow, Y. Rekhter, D. Farinacci, T. Li, and A. Conta Mpls label stack encoding , RFC 3032,, January 2001.
[11] A. Gaeil and C. Woojik Design and implementation of mpls network simulator (mns) supporting qos , 15th International Conference on Information Networking,, January 2001.
[12] A. Gaeil and C. Woojik, Design and implementation of mpls network simulator (mns) supporting ldp and cr-ldp, proceedings of the IEEE International Conference on Networks (ICON 00), September 2000.
[13] A. Gaeil and C. Woojik Simulator for mpls path restoration and performance evaluation, http://flower.ce.cnu.ac.kr/Ë. fog1/mns/index.htm see path protection/restoration, April 2001.
[14] 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.
[15] P. Sakarindr and N. Ansari Security Services in Group Communications Over Wireless Infrastructure, Mobile Ad Hoc, and Wireless Sensor Networks , IEEE Wireless Comm., vol. 14, no. 5, pp. 8-20, Oct. 2007.
[16] A.M. Hegland, E. Winjum, C. Rong, and P. Spilling A Survey of Key Management in Ad Hoc Networks , IEEE Comm. Surveys and Tutorials, vol. 8, no. 3, pp. 48-66, Third Quarter 2006.
[17] L. Zhou and Z.J. Haas Securing Ad Hoc Networks , IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Nov./Dec. 1999.
[18] L. Zhou, B. Cchneider, and R. Van Renesse COCA: A Secure Distributed Online Certification Authority, , ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.
[19] H. Chan, V. Gligor, A. Perrig, and G. Muralidharan On the Distribution and Revocation of Cryptographic Keys in Sensor Networks , Trans. Dependable and Secure Computing, vol. 2, no. 3, pp. 233-247, July 2005.
[20] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, Resisting Flooding Attacks in Ad Hoc Networks, Proc. IntâAZl Conf. Information Technology: Coding and Computing, vol. 2, pp. 657-662, Apr. 2005.
[21] 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. Technology: Coding and Computing, vol. 2, pp. 657-662, Apr. 2005.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)