ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Cluster Based Certificate Revocation and CBRP in Manet

Mathan.S[1], S.Shahul Hammed[2]

Student, Computer science and Engineering, Karpagam University, India[1]

AP, Computer science and Engineering, Karpagam University, India[2]

ABSTRACT: Mobile ad-hoc networks (MANETs) have received increasing attention in recent years due to their mobility feature, dynamic topology, and ease of deployment. However, the wireless and dynamic natures render them more vulnerable to various types of security attacks than the wired networks. The major challenge is to guarantee secure network services. To meet this challenge, certificate revocation is an important integral component to secure network communications. In this paper, a Cluster-based Routing Protocol (CBRP) is proposed to focus on the discovery and maintenance of route more efficiently in Mobile ad hoc networks. The performances of our scheme are evaluated by both numerical and simulation analysis. Extensive results demonstrate that the proposed routing protocol is effective and efficient to guarantee secure communications in mobile ad hoc networks.

I. INTRDUCTION

MOBILE AD-HOC NETWORK (MANET)

A mobile ad-hoc network is a self organized wireless network which consists of mobile devices, such as laptops, cell phones, and PDAs (Personal Digital Assistants), which can freely move in the network. In addition to mobility, mobile devices cooperate and forward packets between each other to extend the limited wireless transmission range of each node by multihop relaying, which is used for various applications, e.g., disaster relief, military operation and emergency communications.

Due to the absence of infrastructure, mobile nodes in a MANET have to implement all aspects of network functionality themselves. They act as both end users and routers, which relay packets for other nodes. Unlike the conventional network, another feature of MANET is the open network environment where nodes can join and leave the network freely. Therefore, the wireless and dynamic natures of MANETs expose them more vulnerable to various types of security attacks than the wired networks.

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 such as prevention, detection, and revocation.

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. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network.

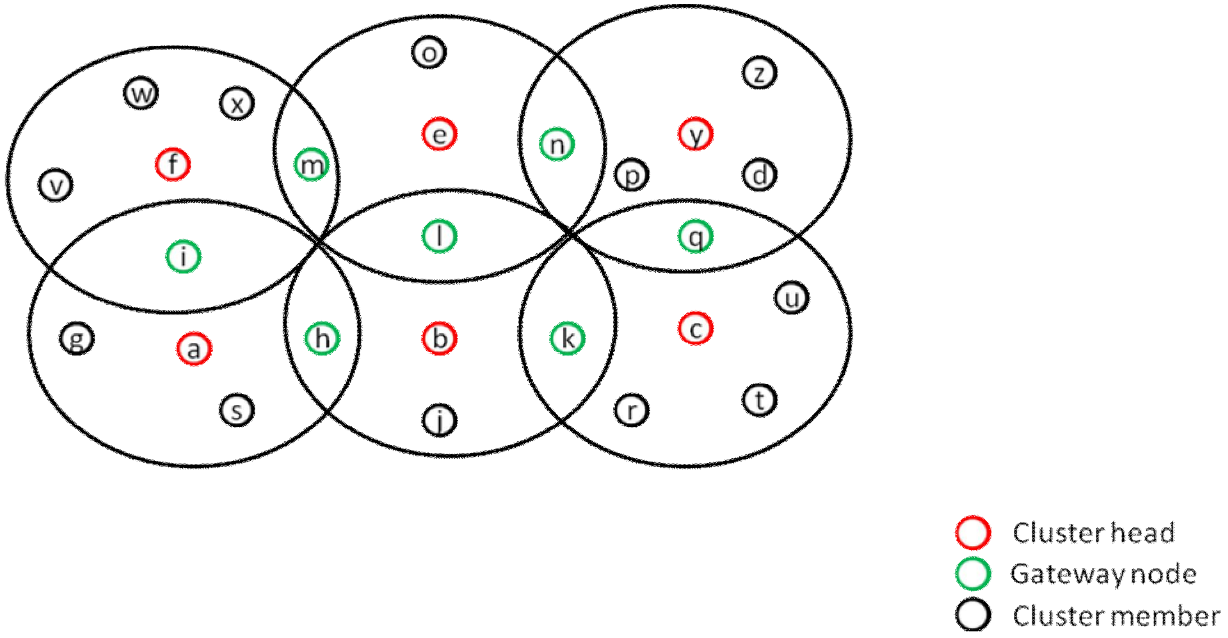
The growth of laptops and 802.11/Wi-Fi wireless networking has made MANETs a popular research topic since the mid 1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

II. NETWORK CREATION

Network creation is the first module of the proposed scheme. It is used to create the network topology. Here N represents the Number of nodes present within the network. If the value of N is not provided then creating network is not possible.

III. CLUSTER FORMATION

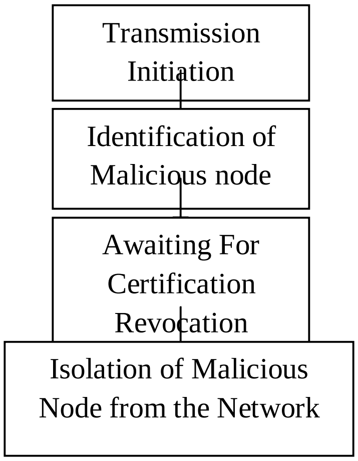
In CBRP the nodes present in a wireless network are divided into several clusters. Each cluster has one node as the cluster head. These cluster heads are responsible for the routing process. A gateway is a node that has two or more cluster heads. Each cluster head has several cluster members. Due to the clustered structure there will be less traffic, because route requests will only be passed between cluster heads.



Cluster structure

IV. CERTIFICATE REVOCATION

After the initiation of transmission the source node will identify whether the neighbour node is malicious or not. If it is a malicious node then it will await for certification revocation. Once the node is revoked then it should remove from the network.


Transmission Initiation
Identification of Malicious node
Awaiting For Certification Revocation
Isolation of Malicious Node from the Network

Flow of certificate revocation

CLUSTER BASED ROUTING PROTOCOL

Route discovery is done by using source routing. In the CBRP, only cluster heads are flooded with route request (RREQ). Gateway nodes receive the RREQs and forward them to the next cluster head. This strategy reduces the network traffic. Once it reach the destination, discard Cluster Head will discard all duplicate RREQs.

V. CONCLUSION

Our proposed algorithm is a Cluster Based Routing Protocol for ad hoc network. By using cluster based routing protocol for routing, it decrease average end-to-end delay and improve the average packet delivery ratio. Cluster head's will discard duplicate RREQ .Once the destination is found, then all RREQ gets drop. The reason is that, routing is depended on the address of cluster heads. By failing any node in the route, its CH may use another node to forward packets (if available). This causes the error tolerance to be enhanced. The performance of proposed protocol is reduce the damage from attacks, attacker node must be immediately removed from the network. By using a Cluster-based Certificate Revocation, the malicious nodes can be revoked from the network.

VI. FUTURE WORK

Packet delivery ratio, Throughput, Packet loss ratio, Security

REFERENCES

1. Wei Liu, Hiroki Nishiyama, Nirwan Ansari, Jie Yang, and Nei Kato, "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks", IEEE Trans. Parallel And Distributed Systems ,VOL.24, NO.2, FEBRUARY 2013.

2. 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.

3. 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.

4. H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "A Dynamic Anomaly Detection Scheme for Aodv-Based Mobile Ad Hoc Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 5, pp. 2471-2481, June 2009.

5. J. Kong, X. Hong, Y. Yi, J.-S. Park, J. Liu, and M. Gerla, "A Secure Ad-Hoc Routing Approach Using Localized Self-Healing Communities," Proc. Sixth ACM Int'l Symp. Mobile Ad hoc Networking and Computing, pp. 254-265. 2005.

6. K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks," Proc. IEEE 71st Vehicular Technology Conf. (VTC '10), May 16-19, 2010.

7. Koushik Majumder, N. Ansari, and N. Kato,"Design and Analysis of the Gateway Discovery Approaches in MANET" Proc. IEEE 61st Vehicular Technology Conf. (VTC '10), March 14-19, 2010.

8. Kuldeep Sharma, Neha Khandelwal, Prabhakar.M, "An Overview Of security Problems in MANET" IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 261-273, Feb. 2006.

9. 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.

10. M. Rezaee, M. Yaghmaee, "Cluster based Routing Protocol for Mobile Ad Hoc Networks" IEEE Trans. Dependable and Secure Computing, vol. 2, no. 3, pp. 233-247, July 2005.

11. 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.