Effect of Malicious Nodes in a Multi-hop Mobile Ad Hoc Network

V.Bhuvaneswari[#1], Dr.M.Chandrasekaran[*2]

[#1]*Department of Computer Engineering*
Government Polytechnic College, Dharmapuri, India
[*2]*Professor & Head, Department of Electronics and Communication Engineering*
Government College of Engineering, Bargur, India

***Abstract*— Providing proper secure communications is challenging in Mobile ad hoc networks (MANETs) because of unreliable wireless media, mobility of the nodes and lack of infrastructure. Usually, wired and wireless networks use cryptographic techniques for secure communications. Symmetric and asymmetric cryptography have been extensively used in Ad hoc networks and have both advantages and disadvantages. Any cryptography becomes weak if it has a weak key management which also forms the main aspect for security in MANETs. Thus, the network is susceptible to attacks by malicious nodes and packets are dropped in attacks like greyhole attack. In this paper, it is proposed to evaluate the performance of a network under the impact of malicious nodes. Greyhole attack was simulated as it is difficult to identify them in the network and their behaviour is also highly unpredictable. Simulations are conducted using DSR routing protocol to evaluate the performance degradation of MANET due to malicious node activity..**

***Keywords*— Mobile Ad hoc Networks (MANETs), Routing, Dynamic Source Routing (DSR), Malicious Nodes, Performance Degradation Introduction**

I. Introduction

Mobile Ad hoc Network (MANET) consists of wireless mobile nodes that communicate with each other without network infrastructure/centralized administration. Mobile hosts are free from any centralized control like base stations/mobile switching centres. Though providing unrestricted mobility and connectivity to users, the onus of network management is entirely on network nodes [1]. Due to the wireless network interfaces limited transmission range, multiple hops are required to exchange data with another across the network. In such networks, each node operates both as host and router, forwarding packets to the other network nodes not within wireless transmission range of each other. All nodes participate in ad hoc routing protocols enabling discovery of multi hop paths to other network .

MANETs are also called infrastructure-less networking, as mobile nodes establish routing among themselves to form networks on the fly. The latter is formed instantaneously using multi-hop routing for information transformation. MANET technology provides a flexible method to establish communication where geographical/terrestrial constraints need a distributed network without a fixed base station like battlefields, military applications, and emergency/disaster situations. A sensor network of numerous small low-powered nodes with sensing capabilities is one of MANET's applications.

Research reveals that wireless MANET has a bigger security problem when compared to traditional wired, and wireless networks [2, 3], though most features make MANETs popular. To begin with in MANETs all signals are routed through bandwidth-constrained wireless links making is liable to many security threats as compared to fixed landline networks and include passive eavesdropping to active interference. Improperly protected mobile nodes can be captured, compromised, and hijacked. Also, an attacker can listen in and modify traffic on wireless communication channel. There are chances that attempts might be made to masquerade as a participant. Authentication - based on public key cryptography and certification authorities – could be hard to accomplish in MANETs because of the lack of infrastructure.

Secondly, as nodes roam freely in any direction security solutions with static configuration are in adequate for a dynamically changing topology. In MANET routing protocols, nodes exchange information about network topology to ensure the establishment of routes between sources and destinations. As messages are transmitted over the air an intruder can maliciously update information incorrectly by pretending to be legitimate. An instance is denial of service (DoS) being launched when a network is flooded with counterfeit routing messages by malicious nodes. Such a message could be forwarded by other innocent nodes.

Third, decentralized decision making in the MANET relies on the cooperative participation of all nodes. The malicious node could simply block or modifies the traffic traversing it by refusing cooperation to break the cooperative algorithms. This property makes some centralized intrusion detection schemes fail. Finally, some/all MANET nodes rely on batteries for their energy. A new type of DoS attack can be created by forcing a node to replay packets to exhaust energy. Due to nodes limited network capacity and battery power, disconnections are frequent in MANETs making identification of anomalies harder.

Generally, wireless MANETs are vulnerable because of their fundamental characteristics which include open medium, dynamic topology, absence of central authority, distributed cooperation and constrained capability. Present security solutions meant for wired networks are inapplicable for wireless MANETs.

Network attacks can be either External attacks or internal attacks. In external attack, the attacker aims to cause congestion, spread false routing information or disturb nodes from providing services. External attacks are attacks launched by challengers who cannot officially participate in the network operations. These attacks usually aim to cause network congestion, deny access to specific network function or to interrupt the whole network operations. External attackers gain access to the network, and once they get access to the network they start sending fake packets, denial of service in order to degrade the performance of the whole network.

In internal attack the attacker wants to have usual access to the network as well as contribute in the normal activities of the network. Internal attack is more severe attacks then external attacks as the attacker uses malicious impersonation to get the admittance to the network as a new node, or by compromising an existing node and using it as a basis to conduct its malicious behaviors. Internal nodes might misbehave to save their limited resources, such as the battery powers, the processing capabilities, and the communication bandwidth. Attacks that are caused by the misbehaving internal nodes are hard to detect because to distinguish between normal network failures and misbehavior activities in the ad hoc networks is not an easy task.

Black hole attack is a common security threat which occurs in MANET. In these attacks, the traffic is redirect to such a node that does not exist in the network. In black hole attack, a malicious node uses its routing protocol to endorse itself as having the shortest route to the destination node. This destructive node advertises its availability of new routes irrespective of checking its routing table. Thus, the attacker node is always to reply to the route request and divert the data packet and retain it. Grey hole is a node that can switch from behaving acceptably to behaving like a black hole.

It has to be understood that security implies identification of potential attacks, threats and vulnerabilities in a system. Karpijoki [2] and Lundberg [4] discussed selected types of attacks possible against a MANET, and they could be classified as passive and active. The former does not disrupt routing protocol operation and only tries to discover information listening to routing traffic and hence is hard to detect. An active attack tries to modify data, gain authentication, or procure authorization through insertion of false packets into data streams/modifying packets transition through networks. Active attack is further categorized into external and internal attacks. The former is caused by nodes strange to a network while the latter is from compromised/hijacked nodes within the network.

Key management is the most crucial one among security issues in MANETs, because it is the assumption of many security services. Secure routing protocols like ARAN [5] and SRP [6], assume that private and public keys and a Trusted Third Party (TTP) signed certificate are assigned to nodes. Research work currently in key management [7, 8] is capable of handling only limited nodes. When this number increases, most are either inefficient or insecure. Also since, MANET has no clearly defined lines of defense; nodes cannot be classified – based on risks - in advance due to MANETs dynamic property. Hence flexibility and adaptability should be considered when planning a key management scheme for MANETs. A major difference between MANETs and wired networks is that in the former, nodes have limited power supplies making redundant any protocol requiring high computation.

Though several security schemes for MANETs were proposed, MANET’s security research is still in its infancy. Transmitting routing information in distributed key management services [9] is through a redundant way so that when a route fails or when limited nodes are compromised, it does not affect the network much. Share refreshing is used to frustrate attacks attempting to discover the certificate authority’s secret key within a limited time as it is felt that the shared signature of the private key of key management services should not be disclosed to an adversary

To counter threats MANETs use mechanisms like IP Security (IPsec), to ensure the security for transmitted data. But before using IPsec nodes should form Security Associations (SAs). During this process, two nodes authenticate one another using certificates, a primary way to verify identities. Key Management Systems create, distribute, and manage such certificates and hence it is the heart of a network’s defenses.

In this paper, it is proposed to evaluate the performance of a network under the impact of malicious nodes. Simulations are conducted using DSR to evaluate the performance degradation of MANET due to malicious node activity. Section 1 dealt with the basics of the wireless network, section 2 reviews some previous works available in the literature. Section 3 details the methods used for evaluation, section 4 gives the simulation result and discusses the same. Section 5 concludes the paper.

II. RELATED WORKS

To form impulsively huge network in MANET using mobile nodes, which is bigger than that of the radio range where the routing supports the communication among each other. Adjih, et al., [10] investigated the issues related to security of MANET and proposed an architecture comprising multiple securing mechanisms is described in detail. OLSR, one of the routing protocols for these types of MANET networks are the main focus in this paper. The proposed architecture mitigates the attacks. Information regarding algorithms, protocols, methods and accomplishment information are provided.

In the current information technology mainly in wireless and mobile environments such as MANETs, key management plays a key role in the security. The dynamic nature of network leads to more concentration on key management as its implementation is very complicated. Based on PKI and identity-based public key cryptography (ID-PKC) are the classical key management approaches that experience the key escrow problem and more cost for computation for certificate verification. Lu Li et al., [11] introduced a new distributed key management approach, which is a combination of certificateless public key cryptography (CL-PKC) and threshold cryptography that retards the single point of failure in addition to the requirement of certificate-based public key distribution and the key escrow problem.

Hadjichristofi et al., [12] proposed a new framework in MANETs for key management which offers robustness and redundancy for the purpose of Security Association (SA) establishment among pairs of nodes. A modified hierarchical trust Public Key Infrastructure (PKI) model is utilized in the proposed KMS where the management roles are assumed by nodes dynamically. The advantages of using the proposed KMS based on the network environment are it maximizes service availability for every nodes, maximizes the accommodating of novel nodes flexibility, reduces pre-configuration, and is able to reconfigure itself dynamically.

Bo Zhu et al., [13] proposed a new hierarchical approach based on threshold cryptography to deal the issue of key management and certification service in MANET considering both security and effectiveness. The contributions of the proposed key management approach comprises: 1) the flexibility to select suitable security configurations in relation to the risks faced is afforded to different parts of MANET, 2) for rapidly-modifying environments, the adaptivity is offered to cope with, 3) MANETs consisting many nodes are handled, 4) with various levels of assurance the certificates are issued. In ad hoc networks to protect certification services from active attacks, two algorithms are additionally proposed that can be employed autonomously from the hierarchical structure. The results obtained by simulating reveals that the 1024 bits key length is around six to eight times faster in the process of renewing or generating a certificate and around 20–80 times faster in the partial certificates generation process. The results obtained by simulating also demonstrate that in a hostile environment where the present methods show weak performance but the proposed two algorithms achieves the best performance. Bing Wu et al., [14] proposed a secure and efficient key management (SEKM) framework. Using a secret sharing scheme and using an underlying multi-cast server groups SEKM builds a public key infrastructure (PKI). Detailed theoretical information in relation to developing and maintaining the server groups is provided. The entire server group forms a view regarding the certificate authority (CA) and offers certificate update service for every node comprising the servers themselves in SEKM. For the purpose of effective certificate service, a ticket scheme is introduced. The proposal introduces an additional efficient server group updating scheme.

III. Results and Discussion

Experiments were conducted with 30 mobile nodes, spread over an area of 2 km by 2 km. The nodes communicate over UPD/IP network. The data rate is uniformly maintained at 11 Mbps for all nodes. The transmission power of 0.005 watts and reception power threshold set at -95dBm is maintained. Simulations are conducted for 5 minutes. Figure 1 shows the scenario without gray hole attack with each node sending data randomly to other nodes in the network with an exponential packet inter arrival time. The size of packets sent is set at exponential (1024).

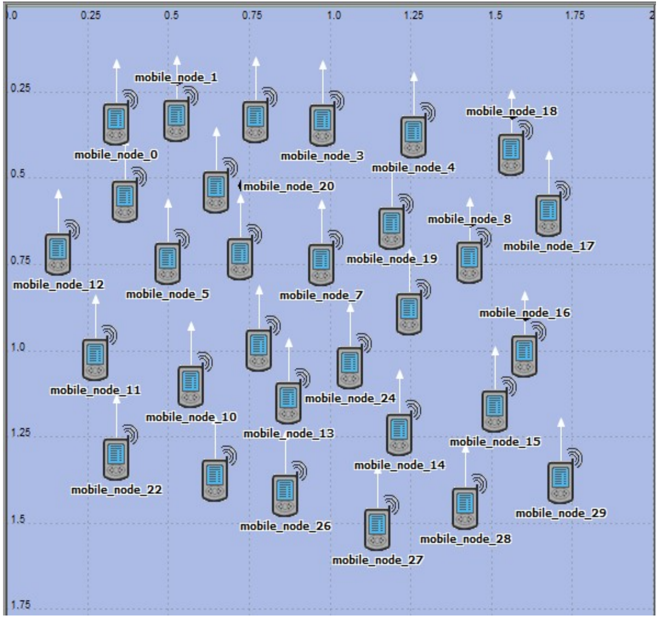

Fig. 1 The network scenario without any malicious nodes.

In the second scenario, five nodes were simulated to perform greyhole attack. The location of the nodes is shown in Figure 2. The malicious nodes are located at the centre of the network for maximum damage. The malicious nodes are designed to randomly drop packets irrespective of the source or destination address.

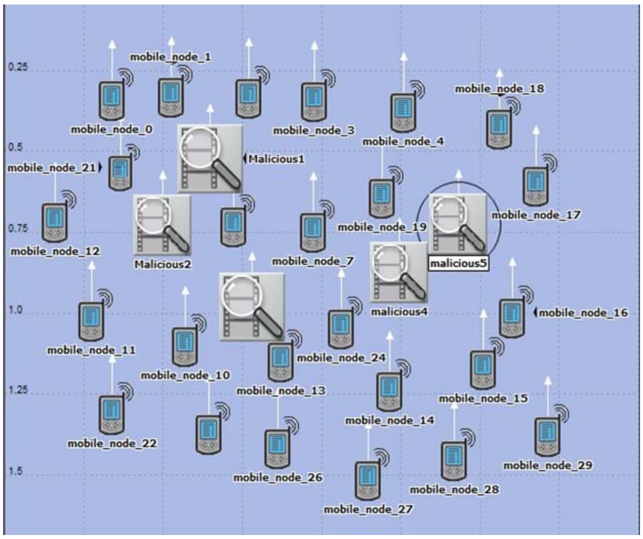

Fig. 2. The network with malicious nodes

Experiments were conducted to simulate the Dynamic source protocol (DSR) with all the nodes cooperating and with 15% (5 nodes) of the nodes being malicious. The attack simulated is grayhole attack. Figure 3 to Figure 5 shows the network performance in terms of successful acknowledgment received, Utilization of route from cache, and throughput respectively. All the outputs plotted are in time average format. Figure 3 shows the total percentage of acknowledgements received within the network for successful data sent.

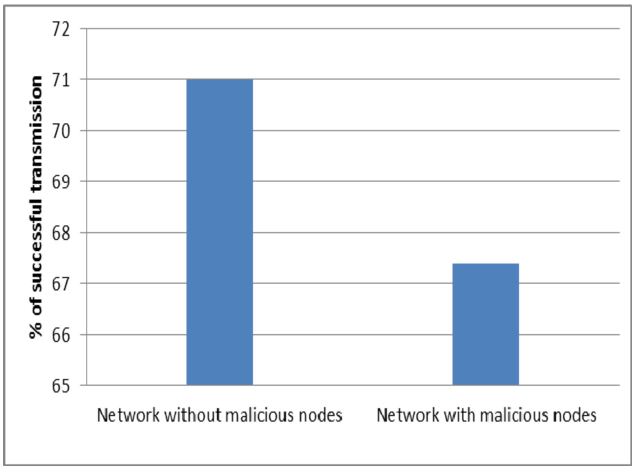

Fig. 3. Successful acknowledgements received

It is seen from Figure 3 that acknowledgments sent when all nodes are cooperating in a network is considerably more when compared to network with malicious nodes. Acknowledgment sent is less in network with malicious nodes as packets are dropped by the malicious nodes during the gray hole attack. Figure 4 shows the average cache utilization for discovering routes.

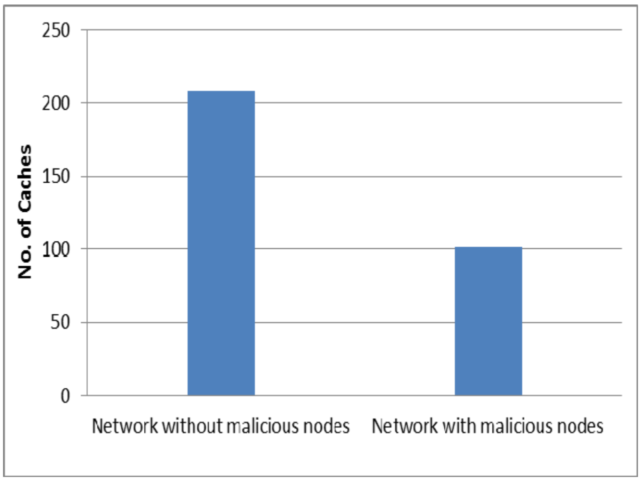

Fig. 4. Utilization of routes from cache

From Figure 4, it can be seen that routes become stale faster in a network consisting of malicious nodes. This is due to the constant packet dropping leading to a new route discovery making the route cache stale. Figure 5 shows the throughput of the system.

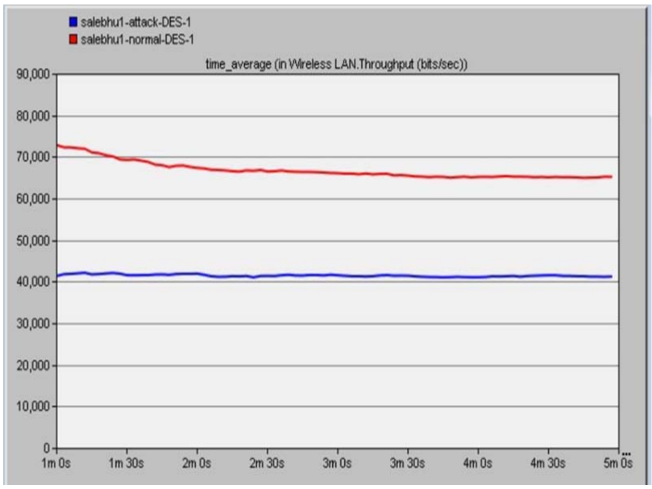

Fig. 5. Throughput in bits/sec for cooperating and malicious network

Due to the presence of 15% malicious nodes the throughput which is the average rate of successful message delivery over the wireless medium of the network decreases by 54.76%. The network degradation is extremely high leading to poor Quality of Service and insecure transmission of data.

IV. CONCLUSIONS

MANETs are susceptible to attacks by malicious nodes and packets are dropped in attacks from malicious nodes. In this paper, it was proposed to evaluate the performance of an Ad hoc network under the impact of malicious nodes. Simulations were conducted using DSR routing protocol to study the performance degradation of the network due greyhole attacks. Simulation was conducted using 30 nodes with 15% of the nodes being malicious and network without any malicious nodes. Simulation results show that the acknowledgments sent, and the various types of route replies are decreased in a network under greyhole attack due to the packet drops. Further investigations to identify malicious node and ways to mitigate them are critical.

REFERENCES

[1] Ci, S., Guizani, M., Chen, H. H., & Sharif, H. (2006). Self-regulating network utilization in mobile ad hoc wireless networks. Vehicular Technology, IEEE Transactions on, 55(4), 1302-1310.

[2] V. Karpijoki, “Security in Ad Hoc Networks,” Seminar on Net Work Security, HUT TML 2000. http://www. hut.fi/~vkarpijo/netsec00/netsec00_manet_sec.ps

[3] L. Zhou and Z. J. Haas, “Securing Ad Hoc Networks,” IEEE Net., vol. 13, no. 6, Nov./Dec. 1999.

[4] J. Lundberg, “Routing Security in Ad Hoc Networks,” Helsinki University of Technology, http://citeseer.nj.nec. com/400961.html

[5] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, A secure routing protocol for ad hoc networks, in: Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP), 2002.

[6] P. Papadimitratos, Z.J. Haas, Secure routing for mobile ad hoc networks, in: SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002.

[7] H. Luo, J. Kong, P. Zerfos, S. Lu, L. Zhang, URSA: ubiquitous and robust access control for mobile ad hoc networks, IEEE/ACM Transactions on Networking 12 (6) (2004) 1049–1063.

[8] Khalili, J. Katz, W. Arbaugh, Toward secure key distribution in truly ad hoc networks, in: IEEE Workshop on Security and

Assurance in Ad Hoc Networks, in Conjunction with the 2003 International Symposium on Applications and the Internet, 2003.

[9] Y. Desmedt, Threshold cryptography, European Transactions on Telecommunications 5 (4) (1994) 449–457.

[10] C. Adjih, D. Raffo, and P. Muhlethaler, “Attacks Against OLSR: Distributed Key Management for Security,” 2nd OLSR Interop/Wksp., Palaiseau, France, July 28–29, 2005.

[11] Lu Li, Ze Wang, Wenju Liu and Yunlong Wang, A Certificateless Key Management Scheme in Moblie Ad Hoc Networks

[12] G. C. Hadjichristofi, W. J. Adams, and N. J. Davis, "A Framework for Key Management in a Mobile Ad-Hoc Network," presented at the International Conference on Information Technology Coding and Computing (ITCC 05), Las Vegas, NV, 2005.

[13] B. Zhu et al., “Efficient and Robust Key Management for Large Mobile Ad Hoc Networks,” Computer Networks, vol. 48, no. 4, July 2005, pp.657–82.

[14] Wu, B., Wu, J., Fernandez, E. B., And Magliveras, S. 2005. Secure and efficient key management in mobile ad hoc networks. In Proceedings of the First International Workshop on Systems and Network Security.