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. 3, Issue 4, April 2015

Study of Standard Techniques for Mitigating the Intrusion Events in Mobile Adhoc Network

Sangeetha.V, Dr. S.Swapna Kumar

Assistant Professor, Dept of CSE, K.S.Institute of Technology, Bangalore, India.

Prof. and Head, Dept of ECE, Vidya Institute of Science & Technology, Trichur, India

ABSTRACT: With the proliferation of Mobile Adhoc Network (MANET) system, the era of networking has undergone massive revolution. But still various issues associated with this types of infrastructureless system are not yet solved effectively. Security is the prime concern for majority of the wireless networking system where the situations turns out more worst when it comes to MANET due to their inherent dynamic topologies. The past decade has seen evolution of massive set of research work that has prioritizes security concern towards safeguarding the communication system over MANET considering various types of attack and intrusion models. However, even with majority of the effective and standards studies on techniques for mitigating security exists, MANET still encounters various types of lethal intrusion threats. This paper consolidates only the effective standard techniques that have been adopted in the past studies.

KEYWORDS : component; Mobile Adhoc Network, Wireless Adhoc, Security, Intrusion.

I. Introduction

In recent years mobile adhoc networks (MANETs) have received tremendous attention because of their self-configuration and self-maintenance capabilities. A Mobile Ad hoc network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies [1][2]. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. Unlike wire line networks, the unique characteristics of mobile ad hoc networks pose a number of non-trivial challenges to the security design.

MANET is characterized by unreliability of wireless links between the nodes, dynamic topology, lack of secure boundaries, threats from compromised nodes inside the network, lack of centralized management, restricted power facilities, and Scalability. Mobile wireless networks are generally more prone to security threats than are fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. Snooping is unauthorized access to another person's data. It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

In network layer wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel. In Black hole attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listen the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply reaches the initiating node before the reply from the actual node, a fake route gets created. Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks.

Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks. Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol. The topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes. Section II discusses about the existing standard techniques followed by prior research work in Section III. Finally, conclusion is discussed in Section IV.

II. EXISTING STANDARD TECHNIQUES

In the previous subsection, we have introduced several well known attack types in the mobile ad hoc network. Therefore, it should be an appropriate time now to find some security schemes to deal with these attacks. In this part, we discuss several popular security schemes that aim to handle different kinds of attack listed in the previous subsection. Intrusion detection is not a new concept in the network research. According to the definition in the Wikipedia, an Intrusion Detection System (or IDS) generally detects unwanted manipulations to systems [3]. Although there are some differences between the traditional wired network and the mobile ad hoc network, intrusion detection technique, which is developed first in the wired network and has become a very important security solution for the wired network, has also gained some attentions from the researchers when they explore the security solution for the mobile ad hoc network. In the following, we discuss some typical intrusion detection techniques in the mobile ad hoc networks in details.

A. *Intrusion Detection Techniques in MANET*:

The first discussion about the intrusion detection techniques in the mobile ad hoc networks was presented in the paper written by Zhang et al. [4]. In this paper, a general intrusion detection framework in MANET was proposed, which was distributed and cooperative to meet the needs of MANET. The proposed architecture of the intrusion detection system is shown below in Figure 1.

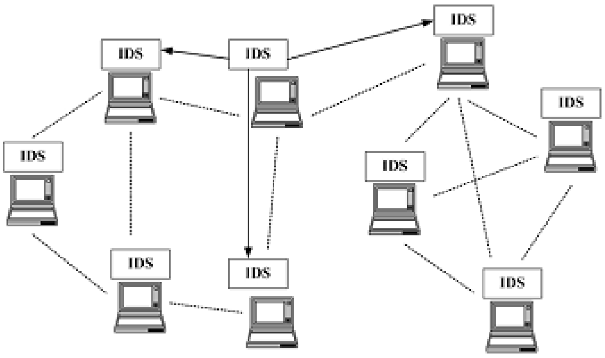

Fig. 1. IDS Architecture for MANET

In this architecture, every node in the mobile ad hoc networks participates in the intrusion detection and response activities by detecting signs of intrusion behavior locally and independently, which are performed by the built-in IDS agent. However, the neighboring nodes can share their investigation results with each other and cooperate in a broader range. The cooperation between nodes generally happens when a certain node detects an anomaly but does not have enough evidence to figure out what kind of intrusion it belongs to. In this situation, the node that has detected the anomaly requires other nodes in the communication range to perform searches to their security logs in order to track the possible traces of the intruder. The internal structure of an IDS agent is shown in Figure 2 below.

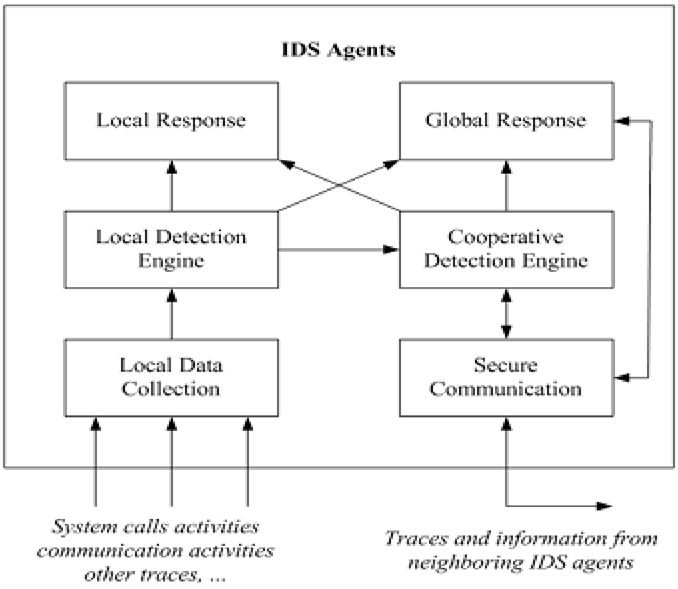

Fig. 2. A Conceptual Model for an IDS Agent

In the conceptual model, there are four main functional modules:

- Local data collection module, which mainly deals with the data gathering issue, in which the real-time audit data may come from various resources.
- Local detection engine, which examines the local data collected by the local data collection module and inspects if there is any anomaly shown in the data. Because there are always new attack types emerging as the known attacks being recognized by the IDS, the detection engine should not expect to merely perform pattern recognition between known attack behaviors and the anomalies that are likely to be some intrusions: instead of the misuse detection technique that cannot deal with the novel attack types effectively, the detection engine should mainly rely on the statistical anomaly detection techniques, which distinguish anomalies from normal behaviors based on the deviation between the current observation data and the normal profiles of the system.
- Cooperative detection engine, which works with other IDS agents when there are some needs to find more evidences for some suspicious anomalies detected in some certain nodes. When there is a need to initiate such cooperated detection process, the participants will propagate the intrusion detection state information of themselves to all of their neighboring nodes, and all of the participants can calculate the new intrusion detection state of them based on all such information they have got from their neighbors by some selected algorithms such as a distributed consensus algorithm with weight. Since we can make such a reasonable assumption that majority of the nodes in the ad hoc network should be benign, we can trust the conclusion drawn by any of the participants that the network is under attack.
- Intrusion response module, which deals with the response to the intrusion when it has been confirmed. The response can be reinitializing the communication channel such as reassigning the key, or reorganizing the network and removing all the compromised nodes. The response to the intrusion behavior varies with the different kinds of intrusion. In the paper, the authors also briefly discuss multi-layer integrated intrusion detection and response technique, in which the intrusion detection module should be set in each layer on each node of the mobile ad hoc network in order to get better performance on some attacks that may seem rather legitimate to the lower layers such as MAC protocol, but are much more easier to detect in the higher layers such as the application layer. The multi-layer integrated intrusion detection and response technique can greatly enhance the performance of the IDS especially when there are large amount of attacks that can be easily caught in the higher layer but are hard to find in

the lower layer. The paper only presents the basic thought of the multi-layer integrated intrusion detection and response technique without providing more specific implementation detail.

This paper explores the intrusion detection techniques in the mobile ad hoc networks. It presents an architecture in which each of the nodes in the mobile ad hoc network should be equipped with an IDS agent, and all of the IDS agents can work independently and locally as well as cooperative with each other to detect some intrusion behaviors in a larger range. In the paper, the authors also describe the conceptual model of the IDS agents and functionalities of different modules in the model. Moreover, the paper also presents an intrusion detection and response scheme in which the IDS agents should be placed in each layer of each node such that some attacks can be detected earlier and more efficiently.

There are two points that this paper does not consider: one is the limited battery power problem that will cause some nodes to behave in a selfish manner during the cooperative intrusion detection process; the other is the possible overhead that is brought by the multi-layer integrated intrusion detection and response mechanism compared with the original single-layer intrusion detection mechanism, or, in other words, what the ratio of the performance enhancement over the overhead increase will be if we apply the multi-layer intrusion detection technique to the MANET. The first point is considered by the authors themselves, which is shown in one of their later papers, and we will discuss that paper in next part. The second point seems not to get enough attention from the researchers, except that there is a preliminary discussion in the paper written by Parker et al. [5], which will also be discussed in this subsection.

B. *Cluster-based Intrusion Detection Technique for Ad Hoc Networks*:

We have discussed a cooperative intrusion detection architecture for the ad hoc networks in the previous part, which was first presented by Zhang et al. However, all of the nodes in this framework are supposed to participate in the cooperative intrusion detection activities when there is such a necessity, which cause huge power consumption for all the participating nodes. Due to the limited power supply in the ad hoc network, this framework may cause some nodes behave in a selfish way and not cooperative with other nodes so as to save their battery power, which will actually violate the original intention of this cooperative intrusion detection architecture. To solve this problem, Huang et al. present a cluster-based intrusion detection technique for ad hoc networks [6].

A MANET can be organized into a number of clusters in such a way that every node is a member of at least one cluster, and there will be only one node per cluster that will take care of the monitoring issue in a certain period of time, which is generally called clusterhead. As is defined in the paper, a cluster is a group of nodes that reside within the same radio range with each other, which means that when a node is selected as the clusterhead, all of the other nodes in this cluster should be within 1-hop vicinity. It is necessary to ensure the fairness and efficiency of the cluster selection process. Here fairness contains two levels of meanings: the probability of every node in the cluster to be selected as the clusterhead should be equal, and each node should act as the cluster node for the same amount of time. Efficiency of the process means that there should be some methods that can select a node from the cluster periodically with high efficiency. The finite state machine of the cluster formation protocol is shown in Figure 3 below.

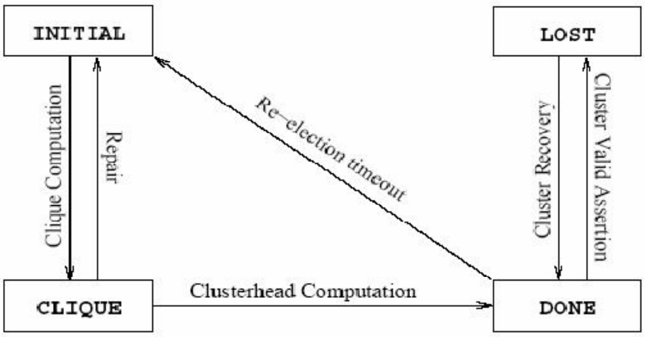

Fig. 3. Finite State Machine of the Cluster Formation Protocol

Basically there are four states in the cluster formation protocol: initial, clique, done and lost. All the nodes in the network will be in the initial state at first, which means that they will monitor their own traffic and detect intrusion behaviors independently. There are two steps that we need to finish before we get the clusterhead of the network: clique computation and clusterhead computation. A clique is defined as a group of nodes where every pair of members can communicate via a direct wireless link. The definition of clique is a little more restricted than that of cluster. The authors use the cluster formation algorithm from [7] to compute cliques, the members of which are named citizens here in the paper. Once the protocol is finished, every node is aware of its fellow clique members. Then a node will be randomly selected from the clique to act as the clusterhead. There are two other protocols that assist the cluster doing some validation and recovery issues, which are respectively called Cluster Valid Assertion Protocol and Cluster Recovery Protocol. The cluster valid assertion protocol has generally been used in the following two situations:

- The node in the cluster will periodically use the Cluster Valid Assertion Protocol to check if the connection between the clusterhead and itself is maintained or not. If not, this node will check to see if it belongs to another cluster, and if it also get negative answer, then the node will enter the LOST state and initiate a routing recovery request.
- Furthermore, there need to be a mandatory re-election timeout for the clusterhead to keep the fairness and security of the whole cluster. If the timeout expires, all the nodes switch from DONE state to INITIAL state and begin a new round of clusterhead election. The Cluster Recovery Protocol is mainly used in the case that a citizen loses its connection with previous clusterhead or a clusterhead loses all its citizens, when it enters LOST state and initiates Cluster Recovery Protocol to re-discover a new clusterhead. In the paper the authors have justified their cluster-based intrusion detection technique by some experiments that make performance evaluation. From the results we can find that the CPU speedup is increased for the cluster-based IDS method than the per-node based IDS method, at the same time the network overhead for the cluster-based IDS methods is lower than that for the per-node based IDS method. However, the detection rate of the cluster-based IDS method is slightly lower than that of the per-node IDS method, which may be reasonable because from a whole cluster point of view, there will only be one node that monitor the traffic for the whole cluster, which can make some inaccurate judgments because of the limited processing power of just one node.

C. *Misbehavior Detection through Cross-layer Analysis:*

Multi-layer intrusion detection technique is another potential research area that Zhang et al. point out in their paper [4]. However, they seem not to explore deeper in this area. In this part, we will discuss the cross-layer analysis method presented by Parker et al. [5]. In this paper, the authors observe the attack behaviors in the MANET, and find that some smart attackers may simultaneously exploit several vulnerabilities at multiple layers but keep the attack to each of the vulnerabilities stay below the detection threshold so as to escape from capture by the single-layer misbehavior detector. This type of cross-layer attack will be far more threatening than the single-layer attack in that it can be easily skipped by the single-layer misbehavior detector.

Nevertheless, this attack scenario can be detected by a cross-layer misbehavior detector, in which the inputs from all layers of the network stack are combined and analyzed by the cross-layer detector in a comprehensive way. The authors also present their attempt by working with RTS/CTS input from the 802.11 MAC layer combined with network layer detection of dropped packets. As far as I know, there are several aspects that can be further explored in this area. First of all, it will be an important problem that how to make the cross-layer detection more efficient, or in other words, how to cooperate between single-layer detectors to make them work well. Because different single-layer detectors deal with different types of attacks, there can be some different viewpoints to the same attack scenario when it is observed in different layers. Therefore it is necessary to figure out the possible solution if there are different detection results generated by different layers. Second, we need to find out how much the system resource and network overhead will be increased due to the use of cross-layer detector compared with the original single-layer detector. Due to the limited battery power of the nodes in the ad hoc networks, the system and network overhead brought by the cross-layer detection should be taken into account and compared with the performance gain caused by the use of cross-layer detection method.

In this part, we survey several typical intrusion detection techniques in the mobile ad hoc networks. Due to the constantly changing topology and limited battery power, the intrusion detection mechanism in the mobile ad hoc networks should be cooperative and energy-efficient, which are shown in the two papers written by Zhang et al. and Huang et al., respectively [4] [6]. Due to the mobility of the nodes and the continuously changing topology in the ad hoc network, it is sometimes relatively hard to collect the enough evidences for a node if it only relies on the single-layer detection method, where it may be vulnerable for the setting of the threshold. As a result, the concept of multi-layer or cross-layer detection mechanism is raised and discussed in [4] and [5]. The intrusion detection mechanisms discussed above contain some good thoughts, which have been proved by the experiments and simulations. However, there are still some problems that need to be further explored in the future.

III. RELATED WORK

The security problem and the misbehavior problem of wireless networks including MANETs have been studied by many researchers e.g. [7], [8], [9], [10]. Although there are number of research conducted in past [11],[12],[13], [14], [15] for analyzing routing attacks on mobile adhoc network. Important routing attacks are fabrication, blackhole, and alteration of various fields in routing packets e.g. RREQ, RREP, RERR message, etc. Research work conducted in [16], [17], [18] discusses about some mitigating techniques for safeguarding the routing protocols in mobile adhoc network. Although these set of research work can successfully resist illegitimate nodes from participating the network, but unfortunately, it was found to increase the significant network overhead with respect to key exchange as well as authentication with restricted intrusion eradication.

In [19] M.K.Jeya Kumar and R.S. Rajesh focused on Cumulative routing Issues. They designed a mobility model using Random waypoint. Using this model AODV performs better than other routing protocols. In [21] Nishu Garg and R.P.Mahapatra worked on Performance degradation due to routing issues. They discussed about security consideration for effective routing, but the result was not optimized. In [22] Dipankar Deb, Srijita Barman Roy and Nabendu Chaki worked on GPS-free positioning systems. They designed Location Aided Cluster Based Energy-efficient Routing and the result obtained here is Lowering mean hop and hence in utilizing the limited energy of mobile nodes. In [23] E.A.Mary Anitan and V.Vasudevan worked on Black hole attack. They Designed Security in Multicast Ad-hoc On Demand Distance Vector for which the result obtained was Better for Black Hole attack. In [24] Ashwani Kush, P. Gupta and C.Jinshong. Hwang worked on Security in Routing protocol. They Designed a Power Aware Virtual Node Routing Protocol but the result was not optimized and it increases Network Overhead. In [25] Sheenu Sharma and Roopam Gupta worked on Black hole attack. Here they worked on measuring the packet loss in the network with and without a blackhole. The result obtained was only 26% reduction in network performance in presence of Blackhole attack. In [26] Cong Hoan Vu and Adeyinka Soneye worked on Collaborative Black hole Attacks. They designed a simulation to check the performance. But the result obtained was resistive against Blackhole attack.

In [27] Irshad Ullah and Shoaib ur rehman worked on Black hole attack. Blackhole attack on OLSR and AODV algorithm was implemented. The result obtained is not effective on DSR, TORA, GRP etc. In [28] Shishir K. Shandilya and Sunita Sahu worked on RREQ Flooding Attack. They designed a distributed cooperative model in which all the node locally run the intrusion detection code and cooperate with each other to detect and prevent flooding attack in the network. The Results obtained was completely dependent on threshold value. The proposed result delays the detection of misbehaving node. In [29] Akanksha Saini and Harish Kumar worked on the effect of Black Hole Attack on AODV. They designed a simulation to check the performance. The experiment didn't reached the better results for ensuring protection from blackhole attack on AODV routing protocol. In [30] Aishwarya Sagar, Anand Ukey and Meenu Chawla worked on Packet Dropping Attack Routing Misbehavior. They Designed a simulation to check the performance and results doesn't guarantee that ACK packets are genuine and no work done in punishing misbehaving nodes. In [31] Moitreyee Dasgupta, Choudhury and Chaki worked on Routing Misbehavior. The impact of rushing attack was implemented by malicious nodes (MNs) on AODV routing protocol. Thye designed RREQ forwarding mechanism for better results. In [31] Kannan and Maragatham worked on Study of various attack. In [33] Amrit Suman worked on Work hole attack. The proposed work was to analyze three ad-hoc routing protocols AODV, DYMO, FISHEYE against wormhole attack in wireless network and obtaine better results.

As seen from literature viewpoint, there are massive work done on securing the routing protocols in MANET, but unfortunately there existing very few schemes that can be considered as benchmarked protocol. The prime reason found behind this is majority of the work has either focused on application view point, or being experimented on some available discrete simulators, or less considerations of problems, usage of much complex cryptography, work towards intrusion detection system and thereby the focus of securing the routing protocol could be furnished much. Hence, the philosophy of our study will be first to design our own simulator which can be customized to any extent and highly applicable for evaluating a large scale MANET

IV. CONCLUSION

In this section, we survey the security solutions in the mobile ad hoc networks. First we analyze the main security criteria for the mobile ad hoc networks, which should be regarded as a guideline for us to find the solutions to the security issues in the mobile ad hoc networks. We then point out various attack types that mainly threaten the mobile ad hoc networks. According to these attack types, we survey several security schemes that can partly solve the security problems in the mobile ad hoc networks. In this survey paper, we try to inspect the security issues in the mobile ad hoc networks, which may be a main disturbance to the operation of it. Due to the mobility and open media nature, the mobile ad hoc networks are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks. First we briefly introduce the basic characteristics of the mobile ad hoc network. Because of the emergence of the concept pervasive computing, there is an increasing need for the network users to get connection with the world anytime at anywhere, which inspires the emergence of the mobile ad hoc network.

However, with the convenience that the mobile ad hoc networks have brought to us, there are also increasing security threats for the mobile ad hoc network, which need to gain enough attention. We then discuss some typical and dangerous vulnerabilities in the mobile ad hoc networks, most of which are caused by the characteristics of the mobile ad hoc networks such as mobility, constantly changing topology, open media and limited battery power. The existence of these vulnerabilities has made it necessary to find some effective security solutions and protect the mobile ad hoc network from all kinds of security risks. Finally we introduce the current security solutions for the mobile ad hoc networks. We start with the discussion on the security criteria in mobile ad hoc network, which acts as a guidance to the security-related research works in this area. Then we talk about the main attack types that threaten the current mobile ad hoc networks. In the end, we discuss several security techniques that can help protect the mobile ad hoc networks from external and internal security threats. During the survey, we also find some points that can be further explored in the future, such as some aspects of the intrusion detection techniques can get further improved. We will try to explore deeper in this research area.

REFERENCES

[1] Ramin Hekmat, Ad-hoc Networks: Fundamental Properties and Network Topologies: “Fundamentals Properties and Network Topologies”, Springer, 01-Sep-2006 - Technology & Engineering - 165 pages

[2] Stefano Basagni, Marco Conti, Silvia Giordano, Ivan Stojmenovic, Mobile Ad Hoc Networking, John Wiley & Sons, 07-Oct-2004 - Technology & Engineering - 416 pages

[3] Intrusion-detection system, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Intrusion-detection_system

[4] Y. Zhang and W. Lee, “Intrusion Detection in Wireless Ad-hoc Networks”, in Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom 2000), pages 275–283, Boston, Massachusetts, August 2000

[5] Jim Parker, Anand Patwardhan, and Anupam Joshi, “Detecting Wireless Misbehavior through Cross-layer Analysis”, in Proceedings of the IEEE Consumer Communications and Networking Conference Special Sessions (CCNC’2006), Las Vegas, Nevada, 2006

[6] Yi-an Huang and Wenke Lee, “A Cooperative Intrusion Detection System for Ad Hoc Networks”, in Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, Fairfax, Virginia, 2003, pp. 135 – 147.

[7] Kejun Liu, Jing Deng, Pramod K. Varshney, and Kashyap Balakrishnan, “An Acknowledgment-Based Approach for the Detection of Routing Misbehaviour in MANETs”, IEEE Transactions on mobile computing, Vol. 6, NO. 5, May 2007.

[8] Dhanalakshmi, Dr.M.Rajaram ,” A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET”, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, Oct2008

[9] Zan Kai Chong, Moh Lim Sim, Hong Tat Ewe, and Su Wei Tan ,” Separation of Detection Authorities (SDA) Approach for Misbehavior Detection in Wireless Ad Hoc Network”,PIERS Online, VOL. 4, NO. 8, 2008.

[10] S. Buchegger and J.-Y. Le Boudec, “Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks,” Proc. MobiHoc, June 2002.

[11] Pradip M. Jawandhiya et. al. / International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4063-4071.

[12] Nishu Garg and R.P.Mahapatra, “MANET Security Issues ,” IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[13] B. Kannhavong, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto. “A study of a routing attack in OLSR-based mobile ad hoc networks”. International Journal of Communication Systems, 20(11):1245–1261, 2007.

[14] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour. "A collusion attack against olsr-based mobile ad hoc networks". In GLOBECOM, 2006.

[15] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour. A Survey of routing attacks in mobile ad hoc networks. IEEE Wireless Communications, page 86, 2007

[16] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing for Ad Hoc Networks," Proc. of MobiCom 2002, Atlanta, 2002.

[17] Y. Hu, D. Johnson, and A. Perrig. SEAD: "secure efficient distance vector routing for mobile wireless ad hoc networks". Ad Hoc Networks, 1(1):175–192, 2003.

[18] Y. Hu, A. Perrig, and D. Johnson. Ariadne:"A Secure On-Demand Routing Protocol for Ad Hoc Networks. Wireless Networks", 11(1):21–38, 2005.

[19] M.K.Jeya Kumar, R.S.Rajesh, "Performance Analysis of MANET Routing Protocols in Different Mobility Models", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.2, February 2009.

[20] Abdul Hadi Abd Rahman, Zuriati Ahmad Zukarnain, "Performance Comparison of AODV, DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc Networks", European Journal of Scientific Research ISSN 1450-216X Vol.31 No.4 (2009), pp.566-576.

[21] Nishu Garg and R.P.Mahapatra, "MANET Security Issues ," IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[22] Dipankar Deb, Srijita Barman Roy, and Nabendu Chaki, LACBER: "A new location aided routing protocol for GPS scarce MANET", International Journal of Wireless & Mobile Networks (IJWMN), Vol 1, No 1, August 2009.

[23] E.A.Mary Anita, V.Vasudevan, "Black Hole Attack on Multicast Routing Protocols", Journal of Convergence Information Technology Volume 4, Number 2, June 2009.

[24] Ashwani Kush, P. Gupta and C.Jinshong. Hwang, "Secured Routing Scheme for Adhoc Networks", International Journal of Computer Theory and Engineering, Vol. 1, No. 3, August, 2009 1793-8201.

[25] Sheenu Sharma, Roopam Gupta, "Simulation study of blackhole attack in the mobile ad hoc networks", Journal of Engineering Science and Technology Vol. 4, No. 2 (2009) 243 – 250.

[26] Cong Hoan Vu, Adeyinka Soneye," An Analysis of Collaborative Attacks on Mobile Ad hoc Networks", Master Thesis Computer Science Thesis no: MCS-2009:4 June 2009.

[27] Irshad Ullah, Shoaib Ur Rehman, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols", Master Thesis Electrical Engineering Thesis no: MEE 10:62 June, 2010.

[28] Shishir K. Shandilya, Sunita Sahu, "A Trust Based Security Scheme for RREQ Flooding Attack in MANET", International Journal of Computer Applications (0975 – 8887) Volume 5– No.12, August 2010.

[29] Akanksha Saini, Harish Kumar, "Effect Of Black Hole Attack On AODV Routing Protocol In MANET", IJCST Vol. 1, Iss ue 2, December 2010.

[30] Aishwarya Sagar, Anand Ukey, Meenu Chawla, "Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010

[31] Moitreyee Dasgupta, S. Choudhury, N. Chaki, "Routing Misbehavior in Ad Hoc Network", 2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 18.

[32] S. Kannan, T. Maragatham, "Attack Detection and prevention methods in Proactive and Reactive Routing protocols", International Business Management 5(3), 2011.

[33] Amrit Suman, Praneet Saurabh, Bhupendra Verma," A Behavioral Study of Wormhole Attack in Routing for MANET", International Journal of Computer Applications (0975 – 8887) Volume 26– No.10, July 2011.