Implemented and Evaluated the Byzantine Attack with the Aid of Rushing Attack in Manet

Neha Agrawal
Mahahrana Pratap College Of Technology
Gwalior
Madhya Pradesh

Krishna Kumar Joshi
Mahahrana Pratap College Of Technology
Gwalior
Madhya Pradesh

Neelam Joshi
Maharana Pratap College Of Technology
Gwalior
Madhya Pradesh

ABSTRACT
The nodes in Mobile Ad-hoc Network(MANET) interacts with one another within the absence of any centralized authority by that the Security is the one of the major problem in MANET. The various security schemes against attack are upgrade the network performance in presence of assaulter to disable misbehavior activity .In this paper we tend to examine the behavior of Byzantine attack result in network that put out infected packets in network that are beyond the capacity of network and apply proffer Intrusion Detection Scheme (IDS) scheme to secure the network from attacker. The proffer IDS scheme is detect the attacker behavior by matching the profile of attacker to normal nodes in network if the profile of nodes are traditional within the foam of correct information delivery in network then the IDS are confirm the network has no attack however if the attack is recognized then IDS has aware of the attacker node in network and additionally managed the profile of attacker and count the infection percentage that infected the network performance. The IDS scheme is 100% recover the network performance as adequate to traditional routing.

General Terms
Mobile Ad-Hoc Network (MANET)

Keywords
Byzantine Attacker, MANET, Security threats, AODV, IDS

1. INTRODUCTION
Wireless ad hoc networks are formed by nodes that are able to communicate with one another using a wireless physical medium without having a pre-existing network framework. This network is known as Mobile Ad hoc NETworks (MANETs). MANETs can be stand-alone group of wireless terminals, but some terminals also connected to fixed networks . An intrinsic characteristic of nodes in ad hoc networks is that they are able to configure the network by themselves and no need to intervention of centralized control. As in wired and configured wireless networks, MANETs are also endangered to security threats. Attacks opposed to routing in MANETs can be divided in to two. An external attack originate from a node (router) that does not involve in the process of routing but facade to be a trusted node. An internal attack originates from node /nodes that take part in the process of routing. The most severe internal attack is byzantine attack, In this attack the data collides in the intermediate nodes ,which forming loops dropping of packets thus degrading the routing services. MANET has come due to potentially rapid infrastructure-less structures in military and extrimity situations. However, the untrustness of wireless links between nodes, feasibility of mobile nodes being seized or compromised, seize up of cooperative algorithms, all lead to increased vulnerability . It is very important to monitor the system and look for intrusions. An IDS forms the second wall of safeguard in the network. Intrusion prevention measures such as authentication and encryption are not guaranteed to work all the time, that brings out the need to complement them with efficient intrusion detection and response. As soon as an intrusion is detected , the intruder can be removed before any damage is done or any data is compromised. Effective IDS not only serve as a deterrent acting to prevent intrusions but also provide information about intrusions to made stronger the intrusion detection and removal methodologies

2. PREVIOUS APPROCHES AND ITS BOTTLENECK
Sharada Valivati et al proposed a method to implement the byzantine rushing attack. This paper focus on Byzantine Flood Rushing attack that threatens the protection of system, and finding out its impact on ad hoc network. The target of task is to implement Flood Rushing attack in AODV enabled ad hoc network . Paper provides an approach to implement and analyze the impact of Byzantine Flood Rushing attack and implementation outcomes are plotted. But it does not suggested any IDS to remove this attack.

Gajendra Singh Chandel et al projected a way for study of rushing attack and implemented the projected techniques over it then compared the outcome of AODV with attack and with prevention technique. In this the result is analyzed by cluster the nodes. This work are often extending to multiple attackers and huge amount of network nodes (50-70 nodes).

Jayashri Padmnabham et all focused on finding routing Black Hole and Byzantine routing attacks by security and trust based mostly routing). Integrity in messages between sender and receiver is achieved via public key crypto graphical method and keyed Hash MAC over a shared secret key. So, that compromising nodes are often detected and ways involving those nodes are neglected.

John S, Baras et all projected a mathematical framework for getting performance bounds of Byzantine attackers and therefore the Intrusion Detection System (IDS) in terms of detection delay. In our formulation we've got on the one hand a bunch of attackers that monitor what's occurring inside the network and coordinate their attack in co-operative manner. On the opposite side, we've a group of preventing nodes (the IDS nodes) that had monitored the network and perform actions against the attackers. This approach ends up in quantifying resiliency of the routing-attack IDS with respect to Byzantine attacks.

Herbert Rubens et all present a detailed description of many Byzantine attacks (black hole, flood dashing, wormhole and

overlay network wormhole), examine their strategies and outline the key reduction technique for it. By simulation, they try to perform a quantitative analysis of the impact of these attacks on an insecure on-demand routing protocol. The strength of the attacks is analyzed by the magnitude of disruption caused per some adversary. An implementation of the On-Demand Secure Byzantine Routing protocol (ODSBR) was created so as to quantify its ability to mitigate the thought of attacks. ODSBR was chosen because its design addresses a large range of Byzantine attacks.

3. PROPOSED WORK

In this thesis , we proposed an innovative approach to detect the severe Byzantine rushing attack. The proposed algorithm is executed on a very popular On Demand Routing Protocol familiar as AODV routing protocol. To implement the effect of the proposed work one of the popular simulators ns-2 is used. The algorithm will detect the malicious node after confirm it as an attack it will removed this attack. We have created a IDS node that captured the path of flowing packets in the network this information is captured before the infected node enters in the network and after the malicious node enter inside network as Byzantine attack, it records the information of normal profile and infect the unsafe node in network through message passing (probing packets) among abstract network and detailed network and then attacker node set the scan rate, scan port, % of vulnerability and infection parameters. If examined port of both networks are same then attacker node sends the infected packets to all the unsafe nodes and infects the network. Intrusion Information catches the information from both normal profile and attacker node and identify the cause of interference, by comparing the information found from both . It examines for fields like attacker node number, port , intrusion time and attack type.

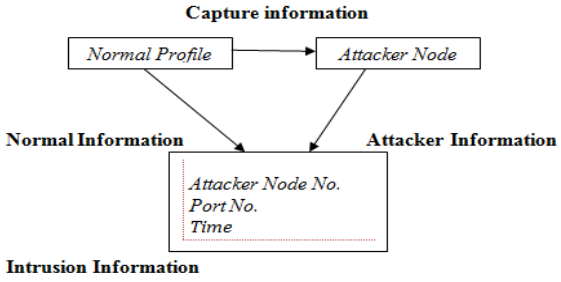


Figure 3.1: Model of Intrusion Detection System

3.1 An IDS (Intrusion Detection System) Algorithm of finding the Byzantine Attack

1. Byzantine attack Mischievousness of nodes may cause severe damage, even can fails whole of the network. In proposed work we have created a new protection scheme against byzantine rushing attacks on nodes. The IDS node recognized the attacker on the basis of profile of nodes in network. If the attacker profile is mismatched with normal nodes and in case of attacker only infection is found.

2. In this scheme we first analyze the routing behavior of malicious nodes against the behavior of byzantine attack and rushing attack, then apply the proper well planned security scheme on it it that restrict the whole misbehavior of malicious nodes and upgrade the network performance.

The Algorithm

Create node =IDS ; // Node as an IDS

Set routing Protocol = AODV;

If ((node is in range) && (next hop !=null))

{

find load (all node)

Create normal_profile();

Create abnormal table();

If ((load < = max_limit) && (ne_ profile == normalprofile()))

{ No attack found;

}

Else

{ Attack in network;

If (new attack == abnormal table())

{

Jam the infected node ;

Find_attack_info(node_number, pkt_type,time)

Capture infection type ;

Infect percentage ;

Port_number ;

}

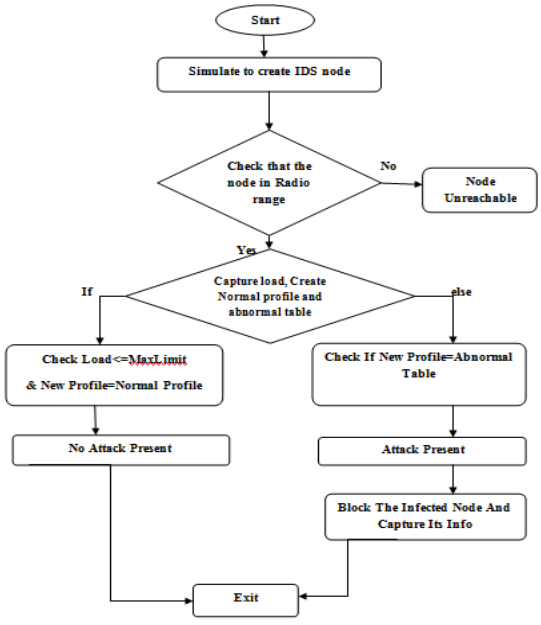
}

Else

{

"Node unreachable"

3.2 Flow chart for the Algorithm



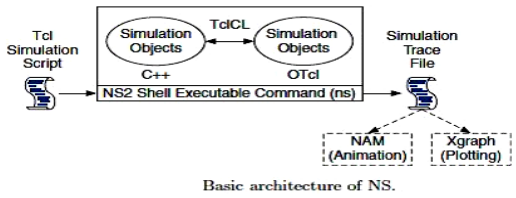
4. SIMULATOR USED

we used one of the most popular and well familiar simulators. called ns-2 (network simulator-2)

4.1 Network Simulator – NS-2

Ns-2 introduced as discrete event simulator for research in networking. It provides significant support for simulation of routing and multicast protocols through cabled and cableless networks. It consists two simulation tools. The network animator (nam) is use to envision the simulations. Ns-2 absolutely simulates a layered network from the physical radio channel to high-level applications. Version 2 is that the most up to date version of ns (ns-2). The simulator was prospered by VINT(Virtual Internetwork test-bed) project group. It supports in the simulation of both type of transport layer, like TCP and UDP, popular MAC layer protocols, a lot of routing protocols over both wired and wireless network etc. The ns-2 simulator has many features that build it suitable for our simulations.

- Provides a network environment for ad-hoc networks,
- Having Wireless channel modules (e.g.802.11),
- Must Routing through multiple ways, and
- Act as Mobile hosts for wireless cellular networks.



Basic architecture of NS.

Figure 4.1: Basic architecture of NS

The simulation results reported in this work, each data point is the average over at least three simulation moves using the same set of parameters.

5. SIMULATION PARAMETERS

Table 6.1 shows simulation parameter here we use routing protocol AODV and analyze effects of byzantine effect (Intrusion) and recovery through IDS Module.

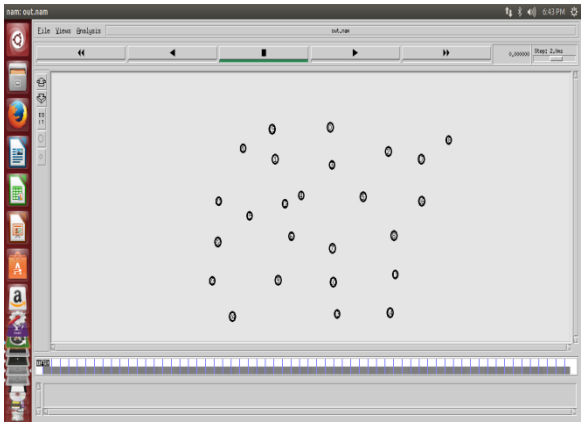
Table 5.1:Simulation Parameters

Parameter	Values
Channel Type	Wireless Channel
Radio-Propagation Model	Two Ray Ground
Network Interface Type	Wireless Phy
Mac Type	802_11
Interface Queue Type	Drop tail/PriQueue
Link Layer type	LL
Antenna Model	OmniAntenna
Max packet in Ifq	50
Number of mobile nodes	25
Routing Protocol	AODV
Time of Simulation End	100ms

6. SIMULATION RESULTS

6.1 Simulation scenario of 25 nodes

In this simulation we construct the mobile ad hoc network contains 25 mobile nodes. The simulation is executed in the NS-2 simulator. The simulation is shown on the NAM(Network Animator)



6.1 Trace File Screenshots

following screenshots are showing the trace file data

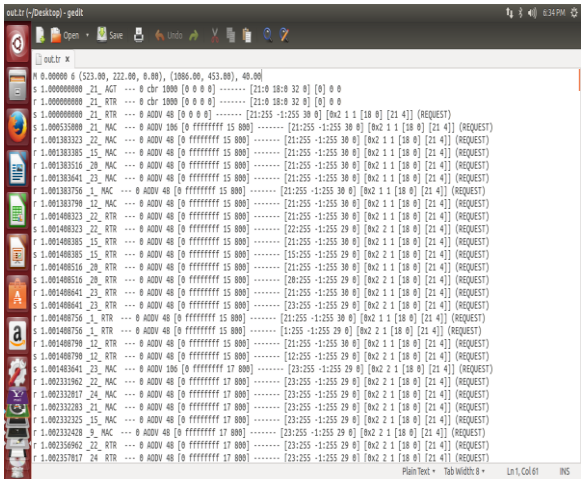


Figure 6.2: A screenshot of Generated Trace File

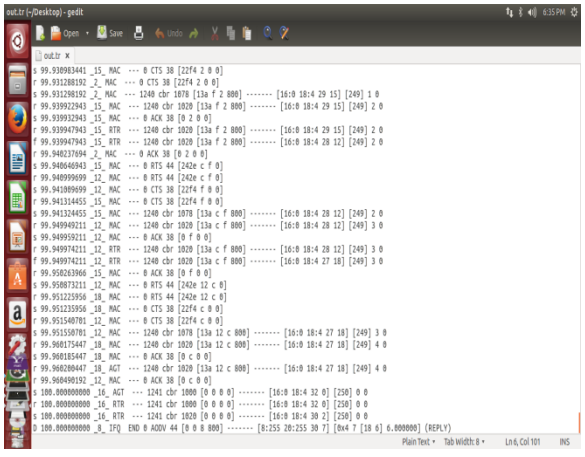


Figure 6.3: A Screenshot of Traffic Generator Script

6.2 NAM Output Screenshots

following screenshots shows the outcome after the simulation have done on the NAM window.

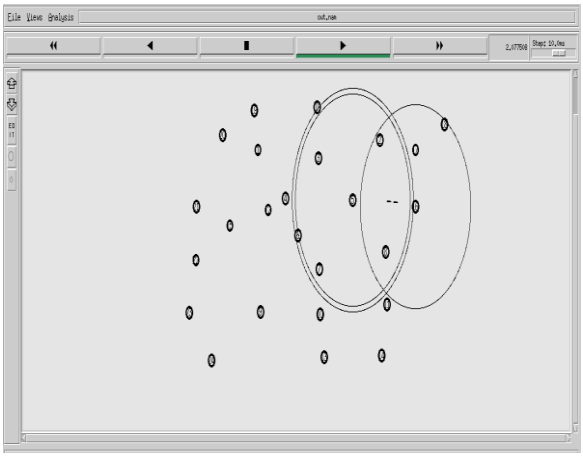


Figure 6.4: A Screenshot of 25 mobile nodes Forwarding The Data Packets

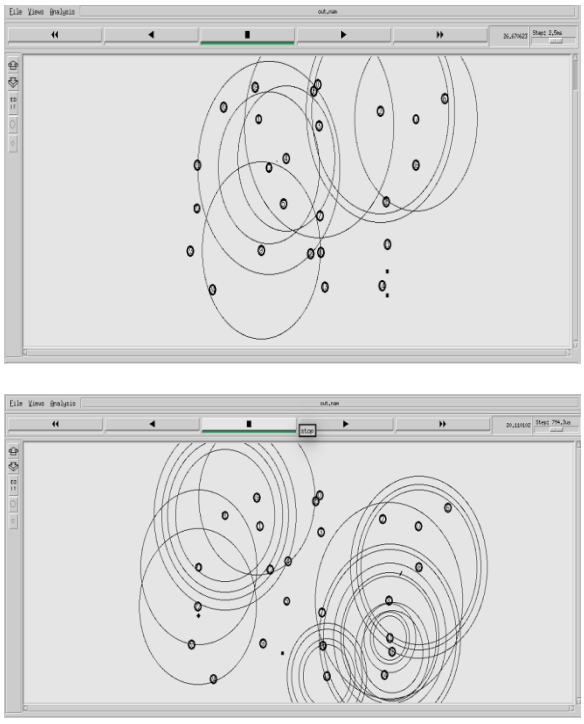


Figure 6.5: The 2 Screenshots Showing The Dropping Of Data Packets At Different Time

7. EXPERIMENTAL EVALUATION OF ATTACK WITH GRAPHS

7.1 Throughput Analysis

This graph represents the throughput analysis within case of normal routing, Byzantine attack and IDS. The throughput has measure on no. of data packets that are received at destination in /sec. At the time of attack throughput decreases due to heavy routing packets flooding in network. But after applying IDS scheme the throughput is equal to normal routing.

following graph shows the throughput of the network

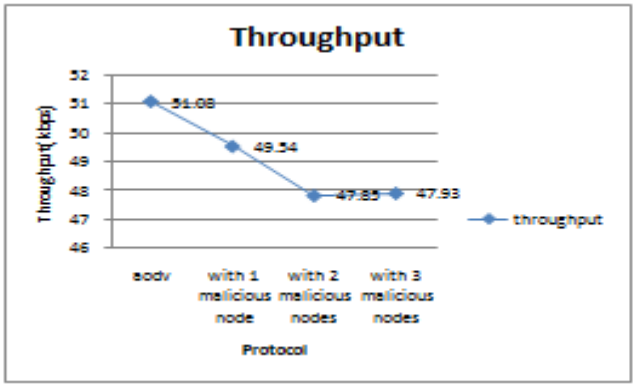


Figure 7.1: Graph Showing the Throughput Analysis

7.2 PDR Analysis

PDF is the ratio of packets received by send packets. The security scheme are improved the performance and providing the efficient PDR in network. So we are showing in the graph for includes without attack and with different number of nodes. But after applying IDS scheme the PDF is equal to normal routing.

following graph shows the PDR of the network

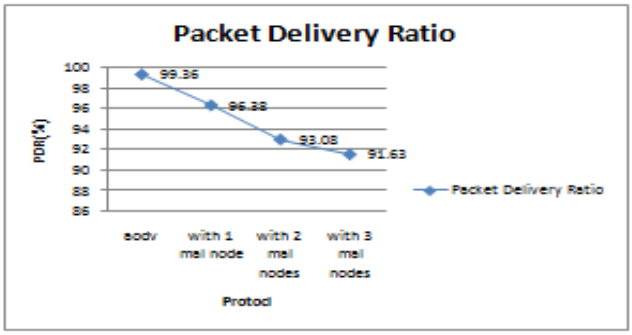


Figure 7.2: Graph Showing The PDR Analysis

7.3 Average end-to-end delay analysis

This metric shows the ratio of the total incoming packets with actual received packets by the end. The following graph shows the avg end-to-end delay with attacks to different no. of nodes. But after applying IDS scheme the Avg end-to-end delay is equal to normal routing.

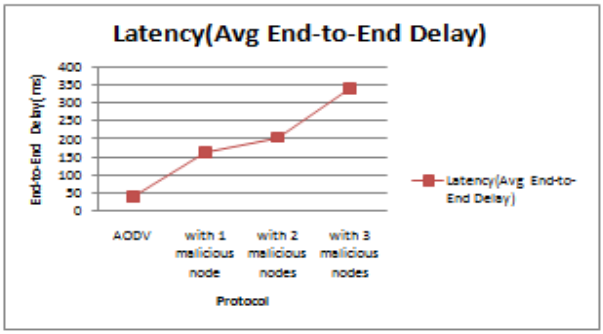


Figure 7.3: Graph Showing The Average End-To-End Delay Analysis

7.4 Overall Analysis

The overall performance of network is shown in table 6.1. This table represents the whole summery of performance metrics in exact figure form means how many packets are send, receive and loss so on in network in case of normal routing, attack and IDS.

Table 7.1 Overall performance of network

Parameters	AODV	Byzantine attack	IDS
Received data	1234	1158	1234
PDR(%)	99.36	93.24	99.36
Throughput(kbps)	51.08	47.93	51.08
End-to-End Delay(ms)	39.57	344.06	39.57

8. CONCLUSION

In this work I analyze and performed the simulation, to evaluate the performance of network using on-demand AODV routing protocols on different parameter performance i.e. packet delivery ratio(PDR) , Throughput and latency with varying different types of parameters.

In this study, we analyzed effect of the Byzantine AODV Network. For this , we implemented an AODV protocol that acts as Byzantine in NS-2. We simulated scenario which have 25 nodes that use AODV protocol and also simulate the same scenario after introducing Three Byzantine Node into the network. Moreover, we also implemented a solution that aim to reduce the Byzantine effects in NS-2 and simulated the solution using the same scenario.

By simulate the Byzantine Attack, we can see that the packet loss is raised in the ad-hoc network. The table of simulation outcome shows the distinction between the number of packets lost in the network with and without a Byzantine Attack. This also shows that Byzantine Attack affects the overall network connectivity and the data loss could show the presence of the Byzantine Attack in the network. If the number of Byzantine Nodes is increased then the data loss would also be expected to increase.

9. FUTURE WORK

We simulated the Byzantine Attack in the Ad-hoc Networks and investigated its affects. In our study, we used the on-demand AODV routing protocol. But also the other routing protocols could be used for simulation as well. All other routing protocols are expected to show different results. So, the best routing protocol for minimizing the Byzantine Attack may be determined.

In our thesis, we try to eliminate the Byzantine effect in the network. But detection of the Byzantine Node is another future work. In our work, we assume the byzantine node is recognized and tried to remove its effects. There are many types of Intrusion Detection Systems in MANET. These IDSs could be tested to find which one is the best to detect the Byzantine.

10. REFERENCES

[1] Sharada Valiveti, Swati R Sharma, Dr. K Kotecha "Performance Evaluation Of Byzantine Flood Rushing Attack In Ad Hoc Network" International Journal of Electronics and Communication Engineering & Technology (IJECET), ISSN 0976 – 6464(Print), ISSN 0976 – 6472(Online), Volume 5, Issue 2, February (2014), pp. 01-09 © IAEME.

[2] Gajendra Singh Chandel, Rajul Chowksi " Effect of Rushing Attack in AODV and its Prevention Technique" International Journal of Computer Applications (0975 – 8887) Volume 83 – No.16, December 2013.

[3] Jayashree Padmanabhan, Tamil Selvan Raman Subramaniam, Kumaresh Prakasam and Vigneswaran Ponpandiyan "A Secure Routing Protocol to combat Byzantine and Black Hole Attacks for MANETs"First International Conference on Advances in Computing and Communications (ACC 2011) Copyright © 2011 ACC Organizing Committee.

[4] A.Rajaram, Dr. S. Palaniswami "Malicious Node Detection System for Mobile Ad hoc Networks" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (2) , 2010, 77-85.

[5] Sunil Taneja and Ashwani Kush "A Survey of Routing Protocols in Mobile Ad Hoc Networks" International Journal of Innovation, Management and Technology vol. 1, no. 3, pp. 279-285, 2010.

[6] John S. Baras, Svetlana Radosavac, George Theodorakopoulos "Intrusion Detection System Resiliency To Byzantine Attacks: The Case Study Of Wormholes In Olsr"IEEE 2007.

[7] B. A. David Holmer, Reza Curtmola, "Mitigating byzantine attacks in ad hocwireless networks", Technical Report Version 1, March 2004.

[8] "http://en.wikipedia.org/wiki/Attack(computing)", August 2012.

[9] C. X. Lujie Zhong, "Byzantine attack with any path routing in wireless mesh networks," IEEE Proceedings of IC-BNMT, vol. 1.0, pp. 711–715, 26-28 Oct 2010. 3rd IEEE International

[10] Conference. *S. E. S. Steven R Snapp, "The distributed intrusion detection system prototype," In*

[11] Proceedings of the Summer USENIX Conference, pp. 227– 233, June 1992.G. F. Calvin Ko, "Automated detection of vulnerabilities in privileged programs by execution monitoring," In Proceedings of the 10th Annual Computer Security Applications Conference, IEEE Computer Society Press, vol. xiii, pp. 134–144, May 1994.

[12] S. C. S. Stani ford Chen, "Grids-a graph based intrusion detection system for large networks," In Proceedings of the 19th National Information Systems Security Conference,*1996.*

[13] G. White and V. Pooch, "Cooperating security managers: Distributed intrusion detectionsystems," Computers & Security, Elsevier Science Ltd., 1996.

[14] F. G. Y. Frank Jou, "Architecture design of a scalable intrusion detection system for theemerging network infrastructure," Department of Com-puter Science, North Carolina StateUniversity, Releigh, N.C, USA, April 1997.

[15] P. A. Porras and P. G. Neumann, "Automated detection of vulnerabilities in privilegedprograms by execution monitoring," In Proceedings of the 10th Annual

Computer SecurityApplications Conference, IEEE Computer Society Press, October 1997.

[16] Cabrera, Gutierrez, and Mehra, "Infrastructures and algorithms for dis-tributed anomalybased intrusion detection in mobile ad-hoc networks," Military Communications Conference, 2005. MILCOM 2005,IEEE, vol. 3, pp. 1831–1837, October 2005.

[17] S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of byzantine attack in large wireless sensor networks," Military Com-munications Conference, 2006. MILCOM 2006, IEEE, pp. 1–4, October 2006.

[18] A. R. Sangi, J. Liu, and L. Zou, "A performance analysis of aodv routing protocol under combined byzantine attacks in manets," Computational Intelligence and Software Engineering, 2009. CiSE 2009, IEEE, vol. 3, pp. 1–5, December 2009.

[19] P. Yi, Y. Wu, and J. Ma, "Experimental evaluation of flooding attacks in mobile ad hoc networks," Communications Workshops, 2009. ICC Workshops 2009. IEEE International Conference, pp. 1–4 ISBN:978–1– 4244–3437–4, 2009.

[20] A. S. ALshahrani, "Rushing attack in mobile ad hoc networks," Third International Conference on Intelligent Networking and Collaborative Systems, pp. 752–758 ISBN: 978– 1–4577–1908–0, 2011.

[21] M. H. Rehmani, S. Doria, and M. R. Senouci, A Tutorial on the Implementation of Ad-hoc On Demand Distance Vector Protocol in Network Simulator. June 2009.

[22] Prof. S.B. Javheri and Shwetambari Ramesh Patil, "Attacks Classification in Network", International Journal of Information Technology and Management Information Systems (IJITMIS), Volume 4, Issue 3, 2013, pp. 1 - 11, ISSN Print: 0976 – 6405, ISSN Online: 0976 – 6413.

[23] Nada M. Badr and Noureldien A. Noureldien, "Review of Mobile Ad Hoc Networks Security Attacks and Countermeasures", International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 6, 2013, pp. 145 - 155, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.