Volume 2, Issue 10 October 2016 ISSN NO: 2454 - 7514

North Asian International Research Journal Consortium

North Asian International Research Journal

Of

Science, Engineering and Information Technology

Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi. All research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

Editorial Board

Address: -North Asian International Research Journal Consortium (NAIRJC) 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815,
Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com

Performance Evaluation for detection of malicious nodes using SVM in MANET

INDERPREET KAUR* & ER.MANASVI MANNAN**

*Research Scholar PCET, Lalru, Punjab

**Astt. Professor PCET, Lalru, Punjab

Abstract

Mobile ad-hoc network has been used in various areas for data transmission over long distances. These nodes have been configured with different movable equipments. There are two types of routing protocols for data communication that are Proactive and Reactive protocol. Proactive protocols are table driven protocol that selects the route from the routing table defined by the user. Reactive protocols are on-demand routing protocols that defines the routing table on time for data transmission. This protocol selects the shortest path for data transmission. Two prevalent on-demand routing protocols which are ad hoc on-demand distance vector (AODV) and dynamic source routing (DSR) protocol are used previously. AODV is constructed based on DSDV routing. In AODV, each node only records the next hop information in its routing table but maintains it for sustaining a routing path from source to destination node. The source node is informed by a route error (RRER) packet first.

Keywords: *MANET, AODV, DSR, Routing protocols, RRER.*

1. INTRODUCTION

1.1 MANET: MANETs are a sort of Wireless specially appointed system that typically has a routable systems administration environment on top of a Link Layer impromptu system. MANETs comprise of a distributed, molding toward oneself, repairing toward oneself system rather than a cross section system has a focal controller (to focus, upgrade, and convey the steering table). A portable specially appointed system (MANET) is a consistently outlining toward oneself, framework less system of cell phones associated without wires. Specially appointed is Latin and signifies "for this reason". Every gadget in a MANET is allowed to move autonomously in any course, and will in this manner change its connections to different gadgets as often as possible.

1.2 MANET's characteristics

1.2.1 Distributed operation: There is no background network for the central control of the network operations; the control of the network is distributed among the nodes. The nodes involved in a MANET should cooperate

with each other and communicate among themselves and each node acts as a relay as needed, to implement specific functions such as routing and security.

1.2.2 Multi hop routing: When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.

3) Autonomous terminal: In MANET, each mobile node is an independent node, which could function as both a host and a router.

1.2.3 Dynamic topology: Nodes are free to move arbitrarily with different speeds; thus, the network topology may change randomly and at unpredictable time. The nodes in the MANET dynamically establish routing among themselves as they travel around, establishing their own network.

1.2.4 Light-weight terminals: In maximum cases, the nodes at MANET are mobile with less CPU capability, low power storage and small memory size.

1.2.5 Shared Physical Medium: The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. Accordingly, access to the channel cannot be restricted.

1.3 Security Attacks in MANET

1.3.1 Passive attack: in this type of attack, the intruder only performs some kind of monitoring on certain connections to get information about the traffic without injecting any fake information. This type of attack serves the attacker to gain information and makes the footprint of the invaded network in order to apply the attack successfully. The types of passive attacks are eavesdropping, traffic analysis and snooping:

1.3.2 Denial of service attack: Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network.

1.3.3 Traffic Analysis: In MANETs the data packets as well as traffic pattern both are important for adversaries. For example, confidential information about network topology can be derived by analyzing traffic patterns. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self-organization in the network, and valuable data about the topology can be gathered. Traffic analysis in ad hoc networks may reveal following type of information.

M ,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.

1.3.5 Active attack: in this type of attack, the intruder performs an effective violation on either the network resources or the data transmitted; this is done by International Journal on New Computer Architectures and Their Applications causing routing disruption, network resource depletion, and node breaking. In the following are the types of active attacks over MANET and how the attacker's threat can be performed [3].

1.3.6 Flooding attack: In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service.

1.3.7 Black hole Attack: Route discovery process in AODV is vulnerable to the black hole attack. In this attack, when a malicious node listens to a route request packet in the network, it responds with the claim of having the shortest and the freshest route to the destination node even if no such route exists. As a result, the malicious node easily misroute network traffic to it and then drop the packets transitory to it.

1.3.8 Active attack: in this type of attack, the intruder performs an effective violation on either the network resources or the data transmitted; this is done by International Journal on New Computer Architectures and

1.3.9 Flooding attack: In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance.

1.3.10 Black hole Attack: In this attack, when a malicious node listens to a route request packet in the network, it responds with the claim of having the shortest and the freshest route to the destination node even if no such route exists. As a result, the malicious node easily misroute network traffic to it and then drop the packets transitory to it.

1.3.11 jamming: Jamming is a special class of DOS attacks which are initiated by malicious node after determining the frequency of communication. In this type of attack, the jammer transmits signals along with security threats. Jamming attacks also prevents the reception of legitimate packets.

1.3.12 malicious code attacks: malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application.

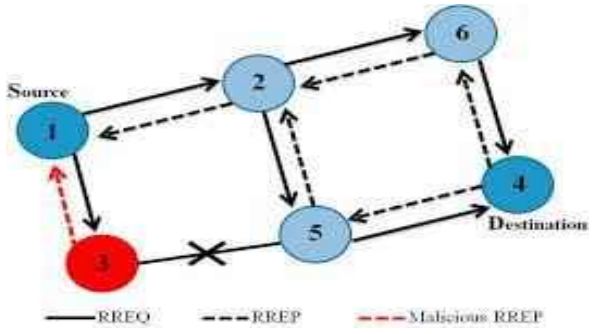

Figure 1.1: Malicious Attack

2. REVIEW OF LITERATURE

Ziming Zhao.et al [1] "Risk-Aware Mitigation for MANET Routing Attacks" Mobile Ad hoc Networks (MANET) have been highly vulnerable to attacks due to the dynamic nature of its network infrastructure. Among these attacks, routing attacks have received considerable attention since it could cause the most devastating damage to MANET. In this paper, we propose a risk-aware response mechanism to systematically cope with the identified routing attacks. Our risk-aware approach is based on an extended Dempster-Shafer mathematical theory of evidence introducing a notion of importance factors. In addition, our experiments demonstrate the effectiveness of our approach with the consideration of several performance metrics.

Shakshuki, E.M. et al [2] "EAACK—A Secure Intrusion-Detection System for MANETs" The migration to wireless network from wired network has been a global trend in the past few decades. In this paper, we propose and implement a new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

Hiranandani, D.et al [3] "MANET protocol simulations considered harmful: the case for benchmarking" In this article, we investigate the current best practices in simulation-based multi-hop wireless ad-hoc network (MANET) protocol evaluation. We extend a prior characterization of the settings and parameters used in MANET simulations by studying the papers published in one of the premier mobile networking conferences between 2006 and 2010. We find that there are still several configuration pitfalls which many papers fall victim to, which in turn damages the integrity of the results as well as any research aimed at reproducing and extending these results.We also propose four "auxiliary" metrics to increase simulation integrity. We conclude with several example scenarios that promote modeling simulations after real-world situations.

Bellavista, P.et al [4] "Convergence of MANET and WSN in IoT Urban Scenarios" Ubiquitous smart environments, equipped with low-cost and easy-deployable wireless sensor networks (WSNs) and widespread mobile ad hoc networks (MANETs), are opening brand new opportunities in wide-scale urban monitoring. Indeed, MANET and WSN convergence paves the way for the development of brand new Internet of Things (IoT) communication platforms with a high potential for a wide range of applications in different domains. Urban data collection, i.e., the harvesting of monitoring data sensed by a large number of collaborating sensors, is a challenging task because of many open technical issues, from typical WSN limitations (bandwidth, energy, delivery time, etc.) to the lack of widespread WSN data collection standards, needed for practical deployment in existing and upcoming IoT scenarios

Gaeta, R. et al [5] "Exploiting Rateless Codes and Belief Propagation to Infer Identity of Polluters in MANET" In this paper, we consider a scenario where nodes in a MANET disseminate data chunks using rateless codes. Any node is able to successfully decode any chunk by collecting enough coded blocks from several other nodes without any coordination. We consider the problem of identifying malicious nodes that launch a pollution attack by deliberately modifying the payload of coded blocks before transmitting. It follows that the original chunk can only be obtained if there are no malicious nodes among the chunk providers. In this paper we propose SIEVE, a fully distributed technique to infer the identity of malicious nodes.

3. METHDOLOGY

Phase 1: In the first phase MANET scenario has been initialized by define the location & mobility of the nodes in the simulation area. These nodes transmit the data from source to destination by using intermediate nodes.

Phase 2: In the second phase of the purposed work malicious nodes have been introduced that perform various attacks like DOS, Blackhole, Gray holes & Selfish node in the environment. In the purposed these attackers' nodes degrades the overall performance of the MANET. This attack has been stating congestion or packet drop.

Phase 3: In the third phase the detection of the malicious nodes available has been clone by computing PDR, PMOR and PMISR. These three factors have been loaded to machine learning

4.RESULTS

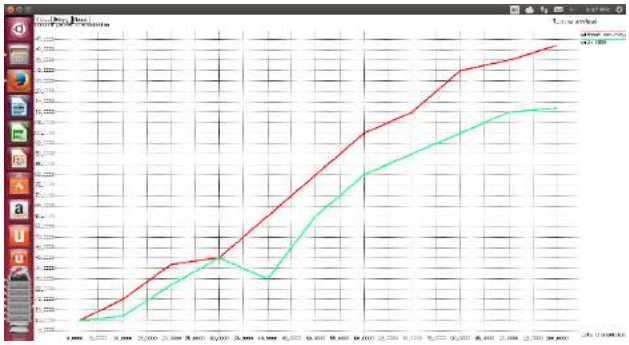

Fig 4.1 Representing overhead

This graph represents routing overhead. Green line represents routing overhead with CBDS and crcn and without CBDS.

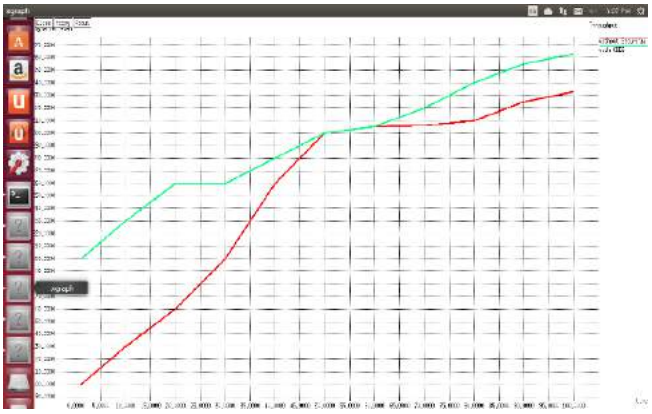

Fig 4.2 Represents throughput

Throughput is total number of successful bites received. This graph represents throughput.

Fig. 4.3 Represents end to end delay

This figure represents end to end delay of nodes. With CBDS delay is lesser as compared to without CBDS hence, after applying CBDS result are better.

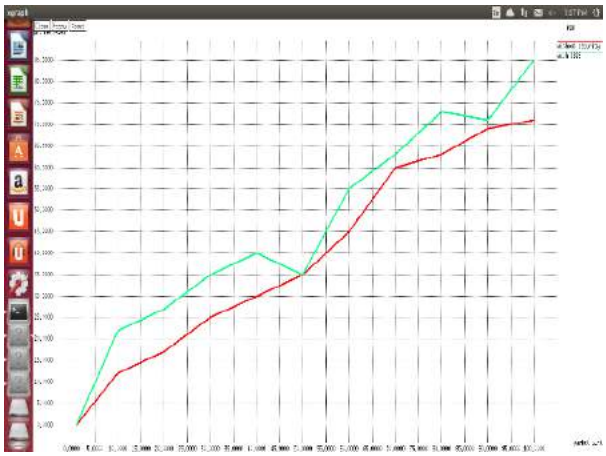

Fig 4.4 Represents PDR

This figure represents PDR (Packet delivery ratio). PDR with CBDS and crcn is good as compared to Without CBDS.

5. CONCLUSION & FUTURE SCOPE

A Mobile Ad-hoc Network (MANET) is a set of remote versatile hubs shaping an element self-sufficient system. Hubs speak with one another without the mediation of concentrated access focuses or base stations. MANETs is Mobile Ad-hoc Network in which nodes are mobile and communicate with each other. It is dynamic topology do not required any central authority. The dynamic topology character of MANETs makes it prone to various

security attacks. Various attack include inside attacks and outside attack. Further these attacks include DOS attack, Alteration attack, Fabrication attack, Black hole attack, Grey hole attack, Wormhole attack, Prankster attack, Sybil attack etc. A malicious attacker can rapidly become a router and break network operations by deliberately not following the protocol specifications. Secure communication is an important aspect of any networking environment, is an especially significant challenge in ad hoc networks. In the previous work a mechanism to detect the wormhole nodes has been proposed by modifying AODV protocol, OLSR protocol, DSDV protocol and DSR protocol. So, in our work to enhance the security we will use TORA Protocol and analyze the system. This scheme helps to secure mobile ad-hoc networks from attacks. We got various parameters and on the basis of these parameters we conclude that our system gives us better results.

In future we can use this approach to analyze performance of others attacks & also some other QOS parameters can be analyzed with large scale networks

REFRENCES

- Burbank, J.L. Johns Hopkins; Chimento, P.F. ; Haberman, B.K. ; Kasch, W. "Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology" journal IEEE on Communications Magazine, Volume 44, 2006,pp-39 – 45.
- Di Crescenzo, G. ; Telcordia Technol., NJ, Ge, R. ; Arce, G.R. "Securing reliable server pooling in MANET against byzantine adversaries" IEEE Journal on Selected Areas in Communications, Volume 24 , 2006,pp-357 – 369.
- Dongkyun Kim, Kyungpook Hanseok Bae. "Improving TCP-Vegas Performance Over MANET Routing Protocols"journal IEEE on Vehicular Technology, Volume 56, 2007,pp- 372 – 377.
- Uichin Lee, Joon-Sang Park, Seung-Hoon Lee, Won W. Ro, Giovanni Pau, Mario Gerla "Efficient peer-to-peer file sharing using network coding in MANET"IEEE Journal on Communications and Networks,Volume10, 2008,pp- 422 – 429.
- El Defrawy, K. Tsudik, G. "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs IEEE Journal on Mobile Computing, Volume10, 2010,pp- 1345 – 1358
- Ziming Zhao; Security Eng. for Future Comput. Lab., Arizona State Univ., Tempe, AZ, USA ; Hongxin Hu ; Gail-Joon Ahn ; Ruoyu Wu "Risk-Aware Mitigation for MANET Routing Attacks" IEEE Journal on Dependable and Secure Computing, Volume 9 , 2011,pp- 250 – 260.
- Shakshuki, E.M. Wolfville, NS, Canada, Nan Kang ; Sheltami, T.R. "EAACK—A Secure Intrusion-Detection System for MANETs" IEEE Journals on Industrial Electronics, Volume 60 , 2012,pp-1089 – 1098.
- Hiranandani, D. Santa Cruz, Santa CruzObraczka, K. ; Garcia-Luna-Aceves, J.J "MANET protocol simulations considered harmful: the case for benchmarking" IEEE Journal on Wireless Communications, Volume:20 , 2013 ,pp- 82 – 90.
- Bellavista, P. Bologna, Italy ; Cardone, G. ; Corradi, A. ; Foschini, L. "Convergence of MANET and WSN in IoT Urban Scenarios" IEEE Journal on Volume 13 , 2013,pp-3558 – 3567.

- Gaeta, R. ; Dipt. di Inf., Univ. di Torino, Turin, Italy ; Grangetto, M. ; Loti, R. "Exploiting Rateless Codes and Belief Propagation to Infer Identity of Polluters in MANET" IEEE_Journal on Mobile Computing, Volume 13, 2013 ,pp- 1482 – 1494.
- Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: Cooperative Bait Detection Approach", IEEE Conf. Malicious Attacks on 2015, pp 65-75.
- K. R. Abirami "An enhanced intrusion detection system for routing attacks in MANET"IEEE International Conference on Advanced Computing and Communication Systems,2013, pp. 1 – 6.
- S. Y. Shin "Wormhole attacks detection in MANETs using routes redundancy and time-based hop calculation" IEEE International Conference on ICT Convergence, 2012, pp. 781 – 786.
- B. Yang "Dempster-Shafer evidence theory based trust management strategy against cooperative black hole attacks and gray hole attacks in MANETs" IEEE International Conference on Advanced Communication Technology,2014,pp. 223 – 232.
- M. Patel "Detection of malicious attack in MANET a behavioral approach" IEEE International Conference on Advance Computing Conference, 2013, pp. 388 – 393.

Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication.

Address:- North Asian International Research Journal Consortium (NAIRJC)
221, Gangoo Pulwama - 192301
Jammu & Kashmir, India
Cell: 09086405302, 09906662570,
Ph No: 01933212815
Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com
Website: www.nairjc.com