Energy Efficiency and Prevention of Packet Dropping Attacks Using IDS Scheme in MANETs

Dr.K.Palanisamy
Assistant Professor, Department of Computer Science
Salem Sowdeswari College (Self), Salem

M.Manikannan
Assistant Professor, Department of Computer Science
Salem Sowdeswari College (Self), Salem

OPEN ACCESS

Volume : 6

Special Issue : 1

Month : September

Year: 2018

ISSN: 2321-788X

Impact Factor: 3.025

Citation:
Palanisamy, K; Manikannan, M. (2018). Energy Efficiency and Prevention of Packet Dropping Attacks Using IDS Scheme in MANETs. *Shanlax International Journal of Arts, Science and Humanities*, 6(S1), pp.41–46.

DOI:
https://doi.org/10.5281/zenodo.1410961

Abstract

A mobile ad-hoc network is an autonomous system, no infrastructure and mobile nodes connected by wireless network. Every mobile nodes in the MANET network is free to move any place and any time any direction in independently. It will change its links to other node continuously. Link and malicious packet dropping are two sources for packet losses in MANET. In the insider-attack case where by malicious nodes that are part of the routing their knowledge of the communication context to selectively drop a small amount of packets less to the network performance. The proposed solution is efficient way to detect and prevention of various packet dropping attacks using Intrusion Detection System (IDS). Sleep scheduling algorithm is used nodes to be awake in a given period same time remaining nodes are in sleep position to minimize energy consumption and enhance the energy efficiency with high performance.

Keywords- IDS, Attacks, Malicious node, DSR, Sleep scheduling, Packet dropping.

Introduction

The MANET is widely used applications of wireless network. It is an self configuring in which collection of mobile nodes cooperate with each other that free to move anywhere and anytime connected by wireless links. Each node in the infrastructure less network that act host and router in the routing time therefore multi-hop packet forwarding in the limited wireless transmission range a node is communicated with other using routing protocol. Dynamic source routing (DSR) is standard reactive routing protocol in MANET. Here DSR is work based on routing discovery and route maintains. In the routing discovery phase the source node broadcasts the route Request (RREQ) packet in the wireless network. Every data packet has the routing path from source to destination in their headers. The source node is send RREQ routing data packet to the destination with the help of routing discovery process when the destination get the routing information then will reply RREP packet to source node.

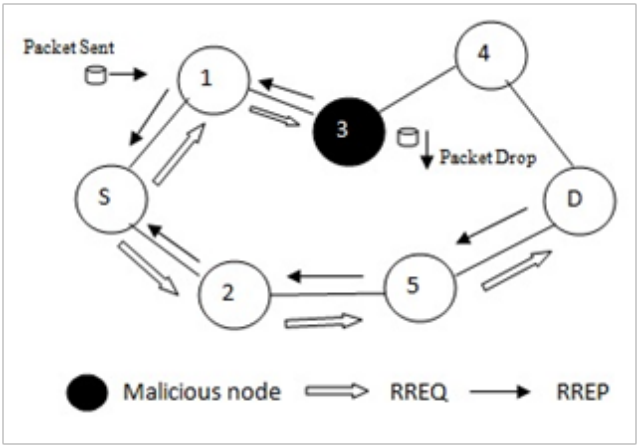

Figure 1 Packet Dropping Attacks

The node's are known each and every intermediate node's address among routing information there is one node connection fails the source node is informed by a route error (RRER) packet. Mobile ad hoc network is not centralized control and its distributed communication system. Thus data transfer between two nodes is requiring security and provide a secure communication to face the security challenges in the MANET. A various of pocket dropping attacks like black hole attack, DOS attack, gray hole and worm hole attacks and etc. Linking error and collaboration of malicious node is source for pocket losses and decrease the network performance in the network. It may disrupt the routing process and the malicious nodes provide fake routing data to the source node whose packets they want to intercept.

Related Work

Jian-Ming Chang et al.[1] proposed a scheme is CBDS for which nodes are malicious activities that attempt to launch collaborative attacks as black hole to detection using a reverse tracing technique. The detected malicious nodes are kept in a black list and other nodes communicate with each other secure routing process that alerted to stop communicating with any node in that list. Weichao Wang et al.[3] propose a new method to generate node of behavioral proofs. Each intermediate node require to consider only a hash calculation for the every received packet. If any nodes are effectively receive the data packets in routing process that time a group of attacker cannot generate its node behavioral proofs. In this new method will accept success to routing segment process for packet drop attacks are detected. It also verify the security and design mechanisms to after reduce the routing overhead on the between nodes. Tao shu et al.[5] proposed an accurate algorithm for detecting selective packet drops made by insider attackers. This algorithm also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. The positions of lost packets as calculated from the auto-correlation function (ACF) of the packet-loss bitmap. A bitmap describing the lost/received status of each packet in a sequence of consecutive packet transmissions and packet-loss bitmaps reported by individual nodes along the route are truthful this can be achieved by some auditing. Bhagyashree et al.[6] proposed the technique called Homomorphic linear authenticator (HLA) based public auditing architecture is developed that allows the detector to verify the truthfulness of the packet loss information reported by nodes. This technique provides privacy preserving collusion proof and incurs low communication and storage overheads. A packet block based mechanism is also proposed to reduce the computation overhead of the baseline scheme which allows one to trade detection accuracy for lower computation complexity.

Proposed Approach

Attacks in MANET Routing Protocol

Mobile ad hoc network is multi hop routing have posible security attacks are passive and active attacks. Passive attacks will do not damage data and it just read data packet in the network. Active attacks can do either internal and external.The attacker will be modifying the data or injecting new malicious data. DSR protocol basically performs two important functions as routing and data forwarding function. Routing discovery process and routing table maintenance activity by routing function. Data forwarding function used forwarding data packets from source to destination. Routing protocol need trusted working network but some various attack launched by misbehaving nodes. Malicious node is attacker node it participate in the routing to disrupt normal operation of network and dropping all received packets using some attacks black hole , gray hole , DOS and etc.

Intrusion Detection System

The propose a detection scheme is called Intrusion Detection System (IDS). It is software application or device that monitors the every host and identify routing misbehavior of malicious node to detect efficiently. Here used DSR protocol that start routing discovery process to connect nearest nodes after allow the source node send data packets to destination in the network. The problem created by notify the information of malicious node to the other node in the routing that drop data packet itself. A host-based IDS is captures local network traffic to the specific host. It is run on individual hosts or devices in MANET. It can analyze activities and monitors on the host after it can determine which node is involved in malicious activities detect to malicious node list and rapidly block a malicious node.

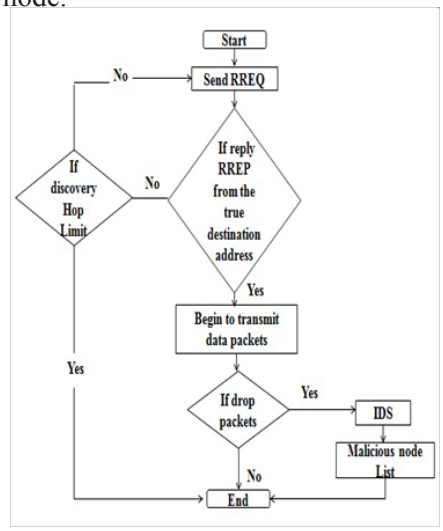

Figure 2 Proposed Methodology

Sleep Scheduling

Mobile nodes are less CPU capability, low storage and small memory size in MANET network. It is called as light weight terminals. It have power conservation because limited battery power that is significantly changed continuously its wireless link. MANET is unsecured boundaries so any time join any node and leave the network so the nodes within network may also behave maliciously. Sleep scheduling is nodes to be awake in a given period while the remaining nodes are in sleep position to minimize energy consumption. Sleep scheduling in mobile ad-hoc networks typically consider on two method as point coverage and node coverage. Point coverage is the awake nodes

are cover specific path or each position of the network in each period. Node coverage awake nodes are globally associated within a network. Sleeping node is an immediate neighbor of at least one awake node. It is based on Geographic Distance Based Neighborhood sleep scheduling algorithm. Source node can select next hop as a neighbor to destination. So many neighbor nodes for a source node and Every node calculates the distance to destination. The source selects a particular node as next node which sends a status message "one" to that particular selected node. This means that the particular node should be in awake mode to receive the packets. All other neighboring nodes get a status message of zero so that they can go to sleep state. After sending the packet, awake node changes to sleep state to save its energy. This process continues until packet reaches the destination. This will improve the scalability and node energy of MANET network.

Simulation Results

The simulation of the proposed methodology is done using the well known network simulator NS-2.34.It is an open source object-oriented discrete-event simulator for network research. The simulator is written in C++ with an OTcl (Object Tool Command Language) interpreter used as the command interface. It is give two output files.

Table 1 Simulation Setup

Parameter	Value
Simulator	NS2
Nodes	30
Area	1000 * 1000
Protocol	DSR
Traffic type	CBR
Simulation time	100 s

They are NAM and tr files.NAM is for visual animation of output and tr is the large text trace file consists of simulation results. In this simulation 30 mobile are considered in the terrain area of 1000*1000.

Packet Delivery Ratio: The ratio between the numbers of packets sends by source nodes to the number of packets correctly received by the corresponding destination nodes.

PDR = received packet/send packet*100

Throughput: The rate of successful delivery of packets over a communication channel. It is usually in kilo byte per second(kbps).

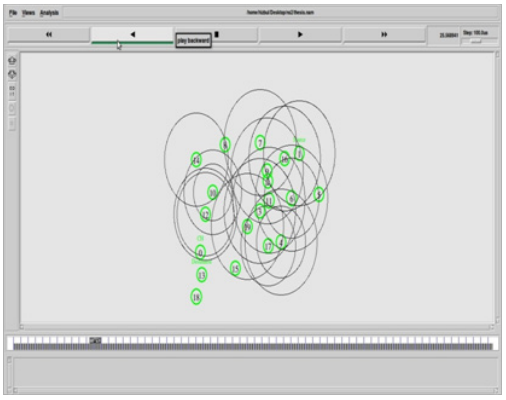

Figure 3 Simulation Result

Conclusion and Future Work

A malicious node is utilizes the routing protocol to falsely replies as having the shortest path to the node then attacker node may free to do incorrupt in the packet will be send by source for the destination. Therefore the network performance is low most packet loss. The present a IDS scheme is effectively detect and remove various packet dropping attacks in the wireless network. Sleep scheduling algorithm can be used sleep-awake cycling is select nodes in the routing path for routing process that nodes are proactive wake up and the energy efficiency with high performance. In the future work the mobility of nodes will be change and more types of attacks including group attacks to the vulnerability of the protocols so find an effective solution to avoid this problem.

References

Aarti,Dr.s.s.Tyagi,"Study of MANET: Characteristics,Challenges,Application and Security Attacks",Volume 3,Issue 5,may2013,ISSN: 2277 12X,Available online at:www.ijarcsse.com.

Abderrahmane Baadache, Ali Belmehdi, " Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.

Anshu Chauhan, D.K. Gupta , Manoj Kumar Sah, " Detection of Packet Dropping Nodes in MANET using DSR Routing Protocol", International Journal of Computer Applications (0975 – 8887) Volume 123 – No.7, August 2015.

Asha L Nair, Dr S.Perumal Sankar, "Sleep Scheduling Technique for Geographic Routing in MANET", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 5, Issue 2, February 2016.

Bhagyashree S and Anand S Uppar " Detection of Malicious Packet Dropping inWireless Ad Hoc Networks Based on Privacy-Preserving Public Auditing" National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)Alva's Institute of Engineering and Technology, Moodbidri Vol. 3, Special Issue 1, April 2015.

David B. Johnson, David A. Maltz ,"Dynamic Source Routing in Ad Hoc Wireless Networks", Computer Science Department, Carnegie Mellon niversity,5000 Forbes A venue Pittsburgh, P A 15213-3891,dbj@cs.cmu.edu.

Fan-Hsun Tseng, Li-Der Chou, Chieh Chao, " A survey of black hole attacks in wireless mobile ad hoc network", Department of Electronic Engineering ,National IIan University, Taiwan.

Jian-Ming Chang (2015), "Defending Against Collaborative Attacks by Malicious node in MANETs: A Cooperative Bait Detection Approach", IEEE SYSTEM JOURNAL. VOL.9.NO.1.

Jian-Ming Chang, Po-Chun Tsou , Han-Chieh Chao and Jiann-Liang Chen ,"CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture".

Ms. Apurva Kulkarni, Mr.Prashant Rewagad, Mr.Mayur Agrawal, "Literature Survey on IDS of MANET", International Journal of scientific research and management (IJSRM) ||Volume||3||Issue||9||Pages|| 3549-3552||2015|| Website: www.ijsrm.in ISSN (e): 2321-3418.

Rashmi Vishwakarma, Moh Imran Hashiam, "An Enhancement of Security level under varying Black Hole attacks in Mobile ad-hoc Network", International Journal of Electrical, Electronics and Comput Engineering4(1): 5765(2015),ISSN No.(Online):2277-2626.

Shweta Gambhir and Kuldeep Tomar,"STUDY OF COMPUTER NETWORK ISSUES ANDIMPROVISING DROP RATE OF TCP PACKETS USING NS2", International Journal in Foundations of Computer Science & Technology (IJFCST), Vol.4, No.4, July 2014.

Sukla Banerjee, " Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

Tao Shu and Marwan Krunz, "Privacy preserving and Truthful detection of packet dropping attacks in wireless Ad Hoc Networks"

Vivek Richhariya,Praveen Kaushik,"A Survey on Network Attacks in Mobile Ad Hoc Networks", Volume 4,Issue 5,may2014,ISSN: 2277 12X,Available online at:www.ijarcsse.com.

Weichao Wang ,Bharat Bhargava, Mark Linderman, " Defending against Collaborative Packet Drop Attacks on MANETs".