Trust Aware Security Based Model for Black-hole and DOS Flooding Attacks in Mobile Ad-hoc Networks: A Survey

[1]Khushbu Upadhyay, [2]Sanjay Bansal, [3]Shaifali Shrivastava
[1,2,3]Dept. of Computer Science, Acropolis Institute of Tech. & Research, Indore, MP, India

Abstract
Dynamic topology, wireless radio medium, limited resources and lack of centralized administration are distinctive features of MANETs, Due to which they are exposed to different types of attacks in different layers of protocol stack. Nodes in a MANET can act as a router. Routing is one of the aspects having various security concerns. Black hole attack and Dos attack which are serious threats for MANETs. On the other hand if the attacker tries to consume resources of the network that degrade the performance of network. Among a number of attacks two serious kinds of attack are considered for demonstrating the proposed fuzzy based trust model for securing the network. The proposed concept's implementation is provided using the Ad-hoc on Demand Distance Vector routing protocol modification in network simulator 2 i.e. NS-2.

Keywords
Security, DOS, Black-hole, NS-2, MANET, Node Communication

I. Introduction

A MANET can be described as a multi-hop temporary communication network of mobile nodes provided with wireless transmitters and receivers without the support of any existing network communications. A MANET is an promising research area with practical applications. However, A MANET is specifically vulnerable due to its fundamental characteristics, such as dynamic topology, open medium, distributed cooperation, and embarrassed ability. Routing plays a significant role in the security of the entire network. Therefore operations in MANETs introduce various new security troubles in accumulation to the ones already present in fixed networks [1]. There are five main security goals that require to be addressed in order to maintain dependable and secure ad-hoc network surroundings. They are mostly [2]:

A. Confidentiality

Securing any information from organism showing to not deliberate entities. In ad hoc networks this is further not easy to absolute because intermediates nodes obtain the packets for additional addressee, so they can simply eaves drop the information organism routed.

B. Availability

Services must be available every time necessary. There must be a declaration of survivability regardless of a Denial of Service attack. On physical and media admission control layer assailant can use jamming method to interfere with communiqué on physical channel. The attacker canister disturbs the routing protocol on network layer. On higher layers, the attacker might communicate down high level services.

C. Authentication

Statement that an origin of communiqué or an entity of concern is what it claims to be or from. With no which an attacker would replicate a node, therefore receiving not suitable admittance to source and sensitive information and intrusive with procedure of additional nodes.

D. Integrity

Message being broadcast is never customized.

E. Non-repudiation

Guarantee that sending and receiving parties can never deny still sending or getting the message.

Type of Security Attacks :

Internal vs. External attacks Internal attacks, in which the adversary needs to contribute in the activities and gain the normal admittance to the network, either by various malevolent impression to get the access to the network as a new node, or by cooperation a present node and using it as a basis to conduct its malevolent behaviors. External attacks, in which the attacker intends to reason congestion, propagate fake routing information or concern nodes from providing services. The security attacks in MANET can be roughly confidential into two major categories, specifically submissive attacks and active attacks are as shown in the fig. 1. The active attacks additional divided according to the layers.

II. Literature Survey

In this paper the author propose the declaration to packet drop attack and development the appearance of network. In this strategy the trusted list is introduced instead of black list. Because the packet drop is insignificant attack as establish to reduce reanalysis overhead analyzed node is or discovery overhead additional to trusted list. So it is skip that node's assessment in prospect. Consequently it is reduce the assessment/calculation or detection overhead for previously analyzed trusted list to some level trusted list is local to every node maintained as data structure in local RAM buffer. Direct reputation technique using two counters [3].
Gayatri Wahaneet. al. proposed a research work that suggests the modification of AODV Routing Protocol. In this paper, security issues of routing in MANETs are discussed in universal, and in exacting the cooperative black hole attack has been described in depth. A security protocol has been future that can be exploiting to recognize multiple black hole nodes in a MANET and thereby identify a safe routing path from a resource node to a purpose node avoiding the black hole nodes [4].
NeetikaBhardwajet. al. presented a new solution to detect and prevent the Black hole which does not increase computation overhead or routing and amplify the presentation metrics like packet delivery ratio, throughput by a large margin. Also the false detection ratio of the approach is negligible. Black hole Attack is one of the most awful attacks because the attacker embeds itself into the route from resource to purpose by sending false RREP messages showing that it has the freshest route to purpose. Seeing its severity various researchers include addressed the problem of

detecting and defending against black hole attack but the resolution obtainable so far suffered from one problem or the other [5].
PoojaJaiswalet. al. proposed a method for finding the secure routes and put off the black hole nodes in the MANET by checking whether there is huge difference between the sequence number of source node before to between node who has sent back RREP or not. In entire the first route reply determine be from the malevolent node with high explanation sequence number, which gets stored because the primary access in the Route Request Table (RRT). Then evaluate the first explanation sequence number with the source node sequence number, if there is additional dissimilarity among them, surely that node is the malevolent node, instantly take away that entry from the RRT [6].
Distributed Denial of Service attacks remain a main security difficulty the mitigation of which is very hard particularly for highly disseminated botnet based attacks. The prior detection of these attacks, though challenging, is essential to protect together end users as well as the limited network communications income. In this paper, we address the difficulty of Distributed Denial of Service attacks and there the theoretical organization, architecture and algorithms of FireCol. The core of FireCol is collected of Intrusion deterrence Systems (IPSs) situated at the Internet Service Providers level. The IPSs form virtual protection rings around the hosts to protect and work together by exchanging chosen traffic information. The estimate of FireCol using universal reproduction and real dataset is obtainable, performance FireCol capability and low overhead, as its support for incremental expenditure in real networks [7].
Distributed Denial of Service (DDos) flood attacks are one of the major concerns for security particular and they are open attempts to dislocate legitimate users' admittance to services. Attackers typically gain admittance to a big number of computers by taking improvement of their vulnerabilities to set up attack armies (i.e., Botnets). In this paper, discover the scope of the Distributed Denial of Service overflow attack difficulty and attempts to combat it. Authors classify the Distributed Denial of Service overflow attacks and categorize obtainable counter measures based on where and while they prevent, perceive, and respond to the DDoS flooding attacks. Additionally, we highlight the required for an inclusive dispersed and collaborative defense approach. The main intention for this work is to kindle the research community into increasing creative, resourceful, efficient, and complete deterrence, discovery, and response apparatus that address the DDoS flooding problem previous to, during as well as after an actual attack [8].
Content-Centric Networking is an emerging networking paradigm being measured as a probable substitute for the current IP-based host-centric Internet communications. Content-Centric Networking focuses on content allotment, which is arguably not efficiently served by IP. Named-Data Networking is an example of CCN. NDN is furthermore an active investigate project under the NSF Prospect Internet Architectures (FIA) program and FIA accentuate security and privacy from the outset and by design. To be a probable Internet architecture, NDN should be bendable against there and promising threats. This paper focuses on dispersed denial-of-service (DDoS) attacks; in thorough we mark interest flood, an attack that increase key architectural features of NDN. We demonstrate that an adversary with finite profits can implement such attack, having a significant impact on network appearance. We then establish Poseidon: a structure for descriptive and detecting interest flood attacks. Lastly, we report on results of universal reproduction estimate future counter estimate [9].

III. Black-hole and Denial of Service Attack

A. Black hole Attack

In Black-hole attack, using routing protocol to an attacker broadcast itself because the shortest pathway to the target device [10]. An attacker watches the routes application in a flood based routing protocol. Still as the attacker receives a application for a route to the target node, it forms a respond concerning of in actuality short route. If the bad respond reaches the initiating node previous to to the reply from the genuine node, a fake route gets created. As malicious device joins the network itself between the communicating nodes, it is brilliant to do every one with the packets going during them. It may crash the packets among them to execute a denial-of-service attack, or on the different use its situation over route is the first step of man-in-the-middle attack [11].
For example, in fig. 1, the resource node S needs to send data packets to purpose node D and initiates the route discovery technique. Assume device 2 is a malevolent device and it claims that it has a route to the reason even as it receives route application packets, and instantly sends the response to node S. If the reply from the malevolent node 2 pressure initially to node S, next node S examine as to route detection is finished, than S ignores all additional replies and start sending data packets to node 2. As an outcome, all packets during the malicious node are compulsive or lost.

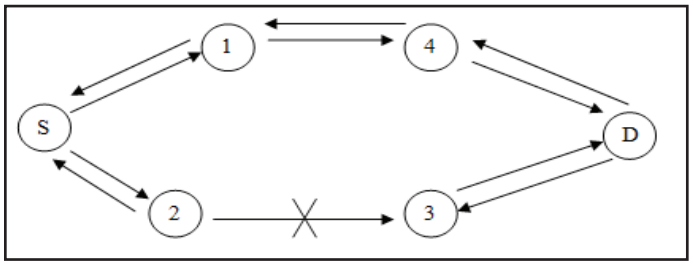

Fig. 1: Black Hole Attack

B. Denial of Service Attack

DOS attacks can reason a critical deprivation of network presentation in conditions of the achieved throughput and latency. The presentation of the wireless network is deteriorate by DOS depends on various factors such as traffic pattern, location of malicious nodes, fairness provided in the network income. It attacks like routing table flood and sleep deficiency fall. The main aim of a DoS attack is the interference of services by attempting to limit access to a machine or service as an alternative of subverting the service itself. This type of attack aims at representation a network incompetent of providing normal service by targeting the networks bandwidth or its connectivity. These attacks achieve their goal by sending at victim a stream of packets that swamps network or indulgence ability denying access to his usual clients. In the not so distant past, there have been big - scale attacks targeting high profile Internet sites [12].

C. Significance of DOS

A common technique of attack involves saturating the target machine with communications requests, by which target machine cannot respond to legitimate traffic, or responds slowly. In other terms, DDoS attacks are deployed by forcing the targeted machine to reset or consuming its resources by which that machine no longer provide its services. There are two chief classes of DDoS attacks: bandwidth depletion and resource depletion attacks [13].

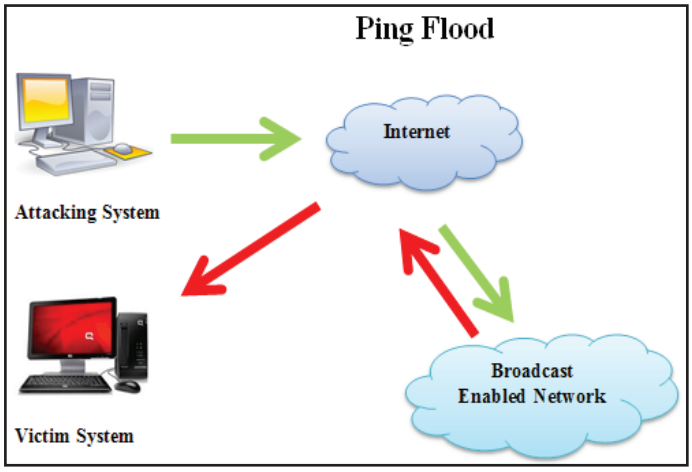

Fig. 2: Denial of Service Attack

D. Bandwidth Depletion

Bandwidth reduction attack will overflow the victim network with unwanted traffic by sending that stops justifiable traffic from accomplishment victim system. Bandwidth attacks can be separated to overflow attacks and magnification attacks.

E. Resource Depletion

Resource depletion attack is an attack that is planned to tie up the income of a victim system. This is done by increasing the TCP protocol and sending will fully inaccurate semantic IP packets to crash the victim system. This kind of attack can be separated to protocol develop attacks and misshapen packet attacks.

IV. Problem Formulation

There are number of trust models for finding the malicious attackers is available and most of techniques are providing solutions for single attack. If the solution is formulated as a framework, to secure the network from more than one attacker using single solution is more effective. Thus an effective technique is required to adopt more parameters by which the other kinds of attackers are also distinguished. The proposed security technique involves the following issues to resolve in the proposed solution.

1. Due to DDOS attacker and Black hole attack injects routing overhead is increases significantly. The routing overhead directly impact on the network performance in terms throughput and packet delivery ratio and end to end delay also.
2. The energy of the network nodes is limited due to the limited power source. The DDOS attacker tries to consume the node energy and Black-hole attacker the data packets. Thus energy consumption is increases and packet delivery ratio becomes too low.

V. Proposed System

The proposed security model is a trust based security framework and promises to provide a secure communication model. Therefore the following security solution is required to implement.

1. To provide efficiency during the route discovery this process is taken place
2. Obtain some essential network parameters that help to design the attribute based rules to improve the performance during the attack.
3. Design of a fuzzy algorithm that helps to identify the Black-hole and DDOS attacks in networks

Algorithm

1: Initialize the network in ideal condition
2: Assign Trust to network via node energy and sending request
3: Calculate Node Trust i.e. Positive and Negative trust
4: Positive trust = 30% energy of node + 70% number of node sending request
5: Negative trust = 1- Positive trust
6: Total trust = Positive trust – Negative Trust
7: Threshold Value =>$\alpha = \frac{1}{N}\sum_{k=0}^{N} Trust$
8: If ($\alpha \geq Each\ node\ trust$)
9: Key set zero i.e. Network is Secure No found malicious
10: Else ($\alpha \leq Each\ node\ trust$)
11: Key set one i.e. Found Malicious

VI. Conclusion

It is easy to deploy DoS flooding and Black-hole attack to impersonate another node in MANET. Mobile ad hoc network has no clear line of defense, so, it is attainable to both legitimate network users and malicious nodes. This survey paper initiate key defense threats in MANET and also explore different Denial of Service attack flooding and Black-hole attack detection and prevention techniques, and how these solutions are capable to safe the network So the finally, by evaluate the advantage and disadvantage of obtainable techniques the open research challenges in mobile ad-hoc network are studied.

References

[1] JunhaiLuo, Mingyu Fan, Danxia Ye,"Black Hole Attack Prevention Based on Authentication Mechanism", The Eleventh IEEE International Conference on Communications Systems (ICCS), pp. 173-177, 2008.
[2] PRADIP M. JAWANDHIYA, MANGESH M. GHONGE and DR. M.S.ALI, "A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology, Vol. 2(9), pp. 4063-4071, 2010.
[3] Ashok M. Kanthe, Ramjee Prasad, Dina Simunic,"The Impact of Packet Drop Attack and Solution on Overall Performance of AODV in Mobile Ad-Hoc Networks", International Journal of Recent Technology and Engineering (IJRTE), Vol. 2, December 2012.
[4] Gayatri Wahane, Prof. Ashok Kanthe,"Technique for Detection of Cooperative Black Hole Attack in MANET", 2014 (ICAET-2014 IOSR Journal of Computer Science (IOSR-JCE) pp. 59-67.
[5] Neetika Bhardwaj, Rajdeep Singh,"Detection and Avoidance of Black-hole Attack in AOMDV Protocol in MANETs", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol. 3, pp. 376-383, 2014.
[6] Pooja Jaiswal, Dr. Rakesh Kumar,"Prevention of Black Hole Attack in MANET", International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol. 2, No. 5, pp. 599-606, Oct 2012.
[7] IssamAib, Raouf Boutaba,"FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks", IEEE/ACM Transactions on Networking, pp. 1828-1841, 2012.
[8] SamanTaghavi Zargar, James Joshi, David Tipper,"A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, pp. 2046-2069, Vol. 15, 2013.

[9] Alberto Compagno, Mauro Conti, Paolo Gasti,"Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking", 38th Annual IEEE Conference on Local Computer etworks, pp. 630-638, 2013.
[10] Shree Om, Mohammad Talib,"Wireless Ad-hoc Network under Black-hole Attack", International Journal of Digital Information and Wireless Communications (IJDIWC) pp. 591-596, 2011.
[11] Juan-Carlos Ruiz, JesúsFriginal, David de-Andrés, Pedro Gil,"Black Hole Attack Injection in Ad-hoc Networks". [Online] Available: http://users.ece.cmu.edu/~koopman/dsn08/fastabs/dsn08fastabs_ruiz.pdf
[12] Douligeris, A. Mitrokotsa,"DDoS attacks and defense mechanisms: Classification and state of-the-art", In Comput. Netw. pp. 643- 666. (Apr. 2004).
[13] Stephen Specht, Ruby Lee,"Taxonomies of Distributed Denial of Service Networks, Attacks Tools, and Countermeasure", Technical Report CE-L2003-03, May 16, 2003.

Ms. Khushbu Upadhyay received her Bachelor of Engineering degree from Mandsaur Institute of technology, Mandsaur in Information Technology in 2007 and ME pursuing from Acropolis Institute of Technology & research, Indore. Her research area include security concern in networking and Data Structure & Algorithm. At present she is a research scholar in network security.

Sanjay Bansal has passed B.E. Engineering) from Shri Govindram Seksariya Institutef Technology and Science, Indore in 1994 and 2001respectively.Presently he is working as Professor at Acropolis Institute of Technology & Researchs research areas are load balanc-ing, fault-tolerance, performance and scalability of distributed system Big Data Data Analytic.

Ms. Shaifali Shrivastava received her BE degree in Information Technology from SIMS in 2010 and ME from AITR, Indore. She was team lead at Magnetic India and currently working as an Assistant Professor in Acropolis Institute of Technology & Research, Indore. Her research interest include Cloud Computing, Linux Operating System and Distributed System. She is 5 times certified in EMC2 ISM/CSI administrator. At present, she is engaged in Programming language & integrated Development Environment (IDEs) in IoT.