RESEARCH ARTICLE OPEN ACCESS

An Efficient Black Hole Attack Detection Using Secure Distributed Path Detection (SDPD) Algorithm

V. Deepadharsini[1], VR.Nagarajan[2]

[1]M.Phil Research Scholar, Department of Computer Science ,Sree Narayana guru College, Coimbatore, India.

[2]Assistant Professor, Department of Computer Science , Sree Narayana guru College, Coimbatore, India.

Abstract:

Secure Routing is a fundamental networking function in all communication system, even multi-hop wireless networks are no exceptions. Attacking the routing service, an adversary can easily paralyze the operation of an entire network. In this research paper aims to present an enhanced Secure Distributed Path Detection (SDPD) Algorithm to prevent the black hole attacks in multi-hop networks. The proposed methodology consists of two important mechanisms, Multipoint Point Relay (MPR) and Shortest path routing. The SDPD is used to select the multiple shortest paths and secure protocol used to transfer a message to destination without packet drops. The path selection is adopted to find the maximum Connection Probability between any given source-to-destination pair in a dynamic way. Through extensive simulations and verification proposed framework achieves extensively better detection accuracy than conventional methods.

Keywords — **MANET, Path detection, Black hole, Attacks.**

I. INTRODUCTION

Mobile ad hoc networks (MANETs) enclose have been an important group of networks, provided that message support in assignment significant scenarios including battlefield and strategic assignments, find and save operations, and tragedy release operations. Cluster infrastructure has been necessary for huge applications in MANETs. The characteristic number of users of MANETs has always increased, and the applications carried by these systems have become increasingly resource demanding. In this turn, has increased the significance of bandwidth effectiveness in MANETs. It is essential for the medium access control (MAC) protocol of a MANET not only to adjust to the dynamic environment but also to efficiently manage bandwidth consumption.

In common, the MAC protocols in wireless networks can be categorized as synchronized and unsynchronized protocols based on the association level [1]. In unsynchronized protocols such as IEEE 802.11, nodes compete with each other to divide the common channel. For the small systems loads the protocols are the bandwidth proficient due to the need of transparency. Though, as the network load boosted, their bandwidth efficiency also decreases.

In a black hole attack [2] a malicious node advertises itself as having a valid route to the destination node even though the route is spurious. With this intension the attacker consumes or intercepts the packet without forwarding it. The attacker can completely suppress or modify the packet and generate fake information, which may cause network traffic diversion or packet drop.

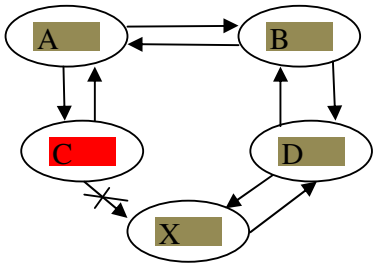

Fig 1: Black hole Attack

The black hole attacks are most often used to publish the addresses of networks linked to spamming; most e-mail server software can be configured to eliminate or flag messages which have been sent from a site listed on one or more such lists.

In figure 1, node "A" wants to send packet to node "X". In order to do so node A will send RREQ message to neighboring nodes i.e. node "B" and node "C". As "C" is malicious node it will quickly responds to the RREQ message send by node "A" by sending a false RREP message. Node "A" will think that it is an active route and will send packet to node "C". After receiving packets from node "A", node "C" will drop all the packets.

All network services of ad hoc network are configured and created on the fly. Thus it is obvious that with lack of infrastructural support and susceptible wireless link attacks, security in ad hoc network becomes inherent weakness [1]. Nodes within nomadic environment with access to common radio link can easily participate to set up ad hoc infrastructure. But the secure communication among nodes requires the secure communication link to communicate. Before establishing secure communication, link the node should be capable enough to identify another node. As a result node needs to provide to identity as well as associated credentials to another node. However delivered identity and credentials need to be authenticated and protected so that authenticity and integrity of delivered identity and credentials cannot be questioned by receiver node. Every node wants to be sure that delivered identity and credentials to recipient nodes are not compromised. Therefore it is essential to provide security architecture to secure ad hoc networking.

The rest of this paper is organized as follows. In Section 2 review the Literature survey. The proposed models and descriptions are described in Section 3. Finally conclude the paper in Section 4.

II. RELATED WORK

In [3] authors addressed the problem of selective jamming attacks in wireless networks. In these attacks, the adversary selectively targets specific packets of "high" importance by exploiting his knowledge on the implementation details of network protocols at various layers of the protocol stack. To illustrated the impact of selective jamming on the network performance by illustrating various selective attacks against the TCP protocol.

In [4] authors addressed the problem of selective jamming attacks in wireless networks. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. To illustrate the advantages of selective jamming in terms of network performance degradation and adversary effort by presenting two case studies; a selective attack on TCP and one on routing

In [5] authors studied the data delivery mechanisms that can with high probability circumvent black holes formed by these attacks. To argued that classic multipath routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. So once the adversary acquires the routing algorithm, it can compute the same routes known to the source, hence, making all information sent over these routes vulnerable to its attacks.

In [6] authors utilized and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all

above requirements. To support efficient handling of multiple auditing tasks, to further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously.

In [7] authors addressed the problem of identifying and isolating misbehaving nodes that refuse to forward packets in multi-hop ad hoc networks. To develop a comprehensive system called Audit-based Misbehavior Detection (AMD) that effectively and efficiently isolates both continuous and selective packet droppers.

In [8] authors proposed a novel method of energy-conserving route protocol called NCE-DSR (Number of times nodes send Constraint Energy DSR). Based on DSR protocol, mark related to the number of times of sending message is added to the datagram for routing protocol. And the nodes with relatively more number of times of sending message are protected. Cost function for route is designed for route choice with reasonable energy allocation for the whole network.

III. RESEARCH METHODOLOGY

The proposed methodology accepts the simulation parameters as input which contains the NS2.34 simulation where the novel Secure Distributed path Algorithm (SDPA) is applied to the mobile adhoc network. This overall proposed architecture in figure 2 follows a routing procedure form start to end state.

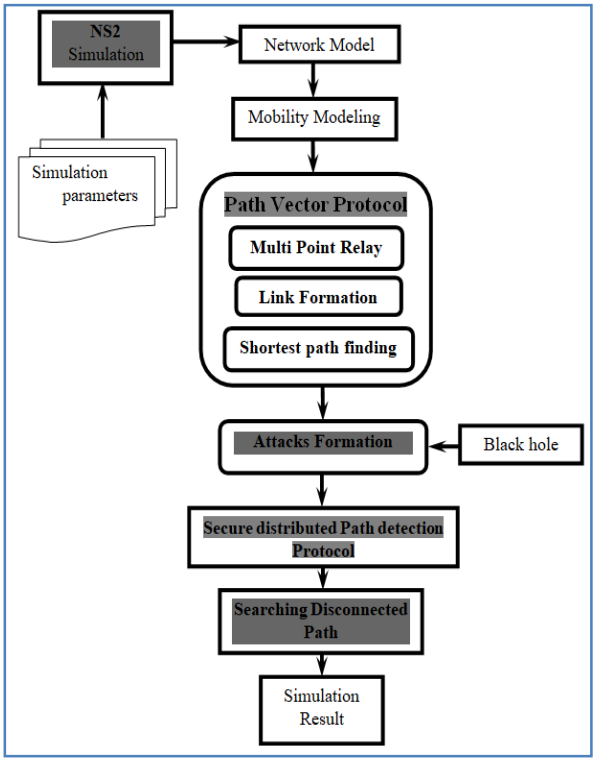

Fig. *2:* Proposed Architecture

A. NETWORK MODEL

The network model in this section concerning the Distributed Path Vector (DPV) protocol is taken from its AODV routing. It is a proactive routing protocol, so the paths are always without delay available when needed. DPV is a normalization model of a pure link state protocol. So the topological changes cause the broadcasting the topological information to all accessible hosts in the network. To reduce the potential collusions in the network protocol uses Multi Point Relays (MPR). The key idea of MPR is to reduce broadcasting public encryption keys in some areas in the network. An additional reduce is to provide by the shortest path. The reducing the time period for the Hello messages transmission can bring more reactivity DPV uses two kinds of the control messages should

be encrypted: Hello and Topology Control (TC). Hello messages are used for searching the information about the connection status and the host's neighbors. With the Hello message the Multipoint Relay(MPR) Selector set is created which describes which neighbors has chosen this host to act as MPR and from this information the host can calculate its own set of the MPRs.

The control messages (Hello messages) are sent only one hop left but the TC messages are broadcasted throughout the whole network. TC messages are used for broadcasting information about own presented neighbors which includes at least the MPR Selector list. The Topology Control messages are transmitted periodically and only the MPR hosts can forward the TC messages.

B. MOBILITY MODELING

In mobility modeling a random waypoint model (RWP) is one of the most extensively used mobility structures in analysis of mobile ad hoc networks. This model analyzes the stationary spatial allocation of a node shifting according to the RWP model in a given convex area. For this it gives an explicit expression, which is in the form of a one-dimensional essential giving the density up to normalization constant. This result is also generalized to the case where the way points have a non-uniform distribution. Additionally, a modified RWP model, where the way points are on the path boundary. The logical results are demonstrated through numerical examples. Additionally, the analytical results are applied to learn certain performance measures in ad hoc networks, namely connectivity and transfer load distribution.

In network simulator (ns-2.34) allocation, the execution of this mobility model is as follows: as the process starts, each mobile node automatically selects one place in the simulation area as the destination. It travels towards this destination with regular velocity chosen consistently and randomly from [0, V], where the parameter V is the maximum permissible velocity for every mobile node. The velocity and orientation of a node are selected independently of other nodes. Upon getting the destination, the node stops for a duration defined by the 'silence time' parameter. If T=0, this leads to continuous mobility. After this duration, it again chooses another casual destination in the simulation field and moves towards it. The entire process is repeated again and again until the simulation process ends.

In the Random Waypoint model, Vmax and Tpause are the two input parameters that determine the mobility actions of nodes. If the Vmax is little and the pause time Tpause is extended, the topology of Ad Hoc network becomes relatively stable. On the other hand, if the node moves fast (i.e.,Vmax is large) and the pause time Tpause is small, the topology is expected to be highly dynamic. Differencing these two parameters, particularly the Vmax parameter, and the Random Waypoint model can generate various mobility scenarios with different levels of nodal speed.

The proposed the Mobility metric to capture and quantify this nodal speed notion. The measure of relative speed between node i and j at time t is,

$$RS(i,j,t) = \left|V_i(t) - \frac{V_j(t)}{M}\right| \quad (1)$$

Then, the Mobility metric is calculated as the measure of relative speed averaged over all node

pairs and over all time. The formal definition is as follows,

$$M = \frac{1}{|i,j|}\sum_{i=1}^{N}\sum_{j=i+1}^{N}\frac{1}{T}\int_{0}^{T} RS(i,j,t)dt \quad (2)$$

where |imp| is the number of distinct node pair (i, j), n is the total number of nodes in the simulation field (i.e., ad hoc network), and T is the simulation time.

Using this Mobility model is able to roughly measure the level of nodal speed and differentiate the different mobility scenarios based on the level of mobility. The Relative Speed (RS) linearly and monotonically increases with the maximum allowable velocity.

C.SECURE ROUTING IMPLEMENTATION

The secure routing of DPV uses two kinds of the control messages: Hello and Topology Control (TC). Hello messages are used for finding the information about the link status and the host's neighbors. With the Hello message the Multi Point Relay (MPR) Selector set is constructed which describes which neighbors has chosen this host to act as MPR and from this information the host can calculate its own set of the MPRs. The Hello messages are sent only one hop away but the TC messages are broadcasted throughout the entire network. TC messages are used for broadcasting information about own advertised neighbors which includes at least the MPR Selector list. The TC messages are broadcasted periodically and only the MPR hosts can forward the TC messages.

The path in the mobile ad hoc network can be either unidirectional or bidirectional so the host must know this information about the neighbors. The control messages are broadcasted periodically for the neighbor sensing. The control messages are only broadcasted one hop away so that they are not forwarded further. When the first host receives the Hello message from the second host, it sets the second host status to asymmetric in the routing table. When the first host send control message and includes that, it has the link to the second host as asymmetric, the second host set first host status to symmetric in own routing table. Finally, when second host send again control message, where the status of the link for the first host is indicated as symmetric, then first host changes the status from asymmetric to symmetric. In the end both hosts know that their neighbor is alive and the corresponding link is bidirectional.

The Control Messages (CM) is used for getting the information about local links and neighbors. The control messages periodic broadcasting is used for link sensing, neighbor's detection and MPR selection process. Control message contains: information how often the host sends control messages, willingness of host to act as a Multi Point Relay, and information about its neighbor. Information about the neighbors contains: interface address, link type and neighbor type. The link type indicates that the link is symmetric, asymmetric or simply lost. The neighbor type is just symmetric, MPR or not a neighbor. The MPR type indicates that the link to the neighbor is symmetric and that this host has chosen it as Multi Point Relay.

D. SECURE DISTRIBUTED PATH DETECTION ALGORITHM

The secure distributed path detection algorithm predicts the distributed attacks (wormhole, grey-hole, and black-hole) in mobile ad hoc network. In

the detection scheme, every node in the network monitors the behavior of its neighbors and upon detecting any abnormal action by any of its neighbors invokes a distributed algorithm to ascertain whether the node behaving abnormally is indeed malicious. The protocol works through cooperation of some security components that are present in each node in the networks. These components are as follows: (i) discovery, (ii) trust collector, (iii) trust manager, (iv) trust propagator. The functions of these components are described below.

The discovery module of each node passively listens to the communication to and from each of its neighbors. For detecting packet drops and modifications by the neighboring nodes, the monitor module of a node randomly copies the incoming packets to its neighbors and checks whether the neighbors really forward the packets with contents unchanged, or drop them, or modify the contents before forwarding them. The collected data is audited by the monitor. The deviation from normal behavior of a neighbor is used as an indicator for the unbiased degree of maliciousness, because this is independent of the past behavior of the neighbor node. If this unbiased deviation exceeds a pre-set threshold, the trust collector module of the node is invoke

The Trust collector module of a node invokes a majority consensus algorithm among the neighbors of a node that has been suspected to be malicious. On being activated by its discovery module, the (accuser) node that has suspected some malicious activity by one of its neighbors challenges the suspicious node to verify its behavior as observed by all of its neighbors. The accused (suspected) node on receiving the challenge responds by acknowledging the message and sending the verify behavior message to all of its neighbors. The neighbors respond by sending the observed value of the degree of maliciousness of the accused node. The accused node calculates the group's trust in its behavior using the received values and broadcasts the computed group-trust along with the received responses to all the neighbors. The messages are also time-stamped so as to prevent replay attacks. For computing group trust value from the received responses, any consensus-based scheme can be used. In the proposed scheme, the difference of the absolute trust values and the average degree of maliciousness of the majority of the respondents (neighbors) has been taken as the final group-trust value of the node. Majority among the neighbors has been taken as the larger of the two subsets of nodes obtained by partitioning the nodes on the basis of a preset threshold value of trust.

Trust Manager: Each node in the network maintains a global trust state containing the suspected nodes and their trust values. A routing table is also maintained that contains a list of nodes that has been determined to be malicious and thus should not be allowed any access to the network resources. The trust manager of a node is responsible for verifying the correctness of the group trust certificate received, caching them, and updating the global trust state (table) of the node for which it has received a new group certificate (from the neighbors of a suspected node). While verifying the correctness, the trust manager must check whether the response from every neighbor node has been correctly considered in computing the group-trust by the suspected node, and the messages have not been tampered with.

The host maintains the routing table, the routing table entries have following information: destination address, next address, number of hops to the

destination and local interface address. Next address indicates the next hop host. The information is got from the topological set (from the TC messages) and from the local link information base (from the Hello messages). So if any changes occur in these sets, then the routing table is recalculated. Because this is proactive protocol then the routing table must have routes for all available hosts in the network. The information about broken links or partially known links is not stored in the routing table.

The routing table is changed if the changes occur in the following cases. Neighbor link appear or disappear, two hops neighbor is created or removed, topological link disappeared or lost or when the multiple interface association information changes. But the update of this information does not lead to the sending of the messages into the network. For finding the routes for the routing table entry the shortest path algorithm is used.

IV. CONCLUSIONS

In this paper, presents an enhanced Secure Distributed Path Detection (SDPD) Algorithm to prevent the black hole attacks in multi-hop networks. s used to select the multiple shortest paths and secure protocol used to transfer a message to destination without packet drops. The path selection is adopted to find the maximum Connection Probability between any given source-to-destination pair in a dynamic way. Through extensive simulations and verification proposed framework achieves extensively better detection accuracy than conventional methods.

REFERENCES

1. Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication," International Journal of Computer Science and Security (IJCSS) Volume: 4 Issue: 3.
2. 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.
3. A. Proano and L. Lazos, "Selective jamming attacks in wireless networks," in Proc. IEEE ICC Conf., 2010, pp. 1–6.
4. A. Proano and L. Lazos, "Packet-hiding methods for preventing selective jamming attacks," IEEE Trans. Depend. Secure Comput., vol. 9, no. 1, pp. 101–114, Jan./Feb. 2012
5. T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.
6. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. IEEE INFOCOM Conf., Mar. 2010, pp. 1–9.
7. Y. Zhang, L. Lazos, and W. Kozma, "AMD: Audit-based misbehavior detection in wireless ad hoc networks," IEEE Trans. Mobile Comput., PrePrint, Vol. 99, published online on 6 Sept. 2013.
8. Linyang Sheng, Jingbo Shao, Jinfeng Ding "A Novel Energy-Efficient Approach to DSR Based Routing Protocol for Ad Hoc Network" 2010 IEEE.