World Research Journal of Telecommunications Systems
ISSN: 2278-8573 & E-ISSN: 2278-8581, Volume 1, Issue 1, 2012, pp.-04-07.
Available online at http://www.bioinfo.in/contents.php?id=357

A NOVEL APPROACH FOR DETECTING AND ESCAPING WORMHOLES IN MANET

GULWADE M.P., DHOOT K.J., BAJAJ A.I. AND PATEL M.M.

Department of Computer Science and Engineering., J.D.I.E.T, Yavatmal, MS, India.
*Corresponding Author: Email- mrunalgulwade@gmail.com, khushboodht@gmail.com, abhishek.bajaj@yahoo.in, majidmpatel@gmail.com

Received: March 06, 2012; Accepted: May 09, 2012

Abstract- Mobile ad-hoc wireless networks are established in improvised environments through the mutual cooperation of its participating nodes. These nodes often operate in a physically insecure environment and, as a result, are vulnerable to capture and compromise. In addition, the nature of the wireless communication medium restricts enforcement of rigorous node memberships and so a number of malicious nodes may also participate in the network. These nodes, in order to snoop or sabotage, can undertake a variety of attacks against the network. Among these wormhole attacks have unusual significance primarily due to their modus operandi and peculiar attack pattern. In such attacks, two or more malicious colluding nodes create a higher level virtual tunnel in the network, which is employed to transport packets between the tunnel end points These tunnels emulate shorter links in the network and so act as bait to unsuspecting network nodes which, by default, seek shorter routes. The benefit gained by the malicious nodes is that they are able to conduct a variety of attacks against the tunneled traffic. In this paper, a novel trust-based scheme for identifying and isolating nodes that create a wormhole in the network, without engaging any cryptographic mean is proposed.
Key words- Ad-hoc, attacks, network, routing protocol, security, trust.

Citation: Gulwade M.P. et al (2012) A Novel Approach for Detecting and Escaping Wormholes in MANET. World Research Journal of Telecommunications Systems, ISSN: 2278-8573 & E-ISSN: 2278-8581, Volume 1, Issue 1, pp.-04-07.

Introduction

In recent years, the explosive growth of mobile computing devices, which mainly include laptops, personal digital assistants (PDAs) and handheld digital devices, has impelled a revolutionary change in the computing world. Computing will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society. In the ubiquitous computing environment, individual users utilize, at the same time, several electronic platforms through which they can access all the required information whenever and wherever they may be. The nature of the ubiquitous computing has made it necessary to adopt wireless network as the interconnection method. It is not possible for the ubiquitous devices to get wired network link whenever and wherever they need to connect with other ubiquitous devices. The Mobile Ad Hoc Network [2] is one of the wireless networks that have attracted most concentrations from many researchers.

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies [6]. People and vehicles can thus be internet worked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network [1], therefore this kind of wireless network can be viewed as mobile ad hoc network.

Dynamic Source Routing and Wormhole Attack

DSR [4] is one of the most widely used reactive protocols in ad-hoc networks. DSR uses two kinds of messages known as RREQ - Route Request and RREP - Route Reply for route discovery process.DSR uses the RREQ message if and only if there are no

routes available in the route cache to reach the destination. DSR starts the route discovery by sending Route Request (RREQ) packet. The RREQ will be uniquely identified by the sequence number, source id and destination id [4]. Node A initiates the route discovery by broadcasting the RREQ message. Each node will then add their id to the route and broadcasts it again. The nodes B, C, D are intermediate nodes and they do not have any source route to reach the node 8, which is the intended destination. The intermediate node which has the route to the destination will send a Route Reply (RREP) and if no intermediate node has the information, the RREQ will be propagated to the destination. The Fig (**1**) depicts the RREP propagation from the destination node E to the source node A. Bogus RREQ will be used to carry out the sinkhole attack. If the bogus RREQ has higher sequence number than the sequence number of the original RREQ from the target node, the intermediate nodes will treat the bogus one as the latest request and discard the original one. The attacks such as black-hole, wormhole, misdirection, and replay can cause an existing route to be broken or a new route to be prevented from being established. Among these attacks wormhole attack is hard to detect because this attack does not inject abnormal volumes of traffic into the network. In a wormhole attack, attackers "tunnel" packets to another area of the network bypassing normal routes as shown in Fig. 1.

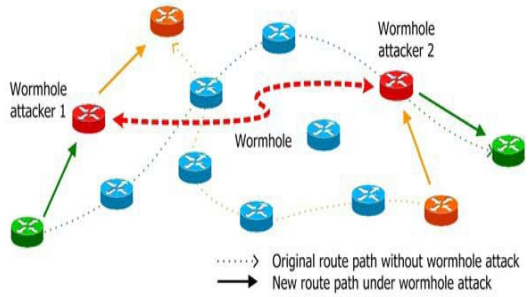

Fig. 1- Illustration of Wormhole Attack in Wireless Network

Trust-Based Wormhole Detection and Evasion in DSR (Dynamic Source Routing) Protocol

Wormhole Creation

In the Tunnelling of packets above the network layer type of wormhole, all packets which are received by a malicious node are duly modified, encapsulated in a higher layer protocol and dispatched to the colluding node using the services of the network nodes. These encapsulated packets traverse the network in the regular manner until they reach the collaborating node. The recipient malicious node, extracts the original packet, makes the requisite modifications and sends them to the intended destination. In this paper, solutions to this type of wormhole is proposed. In an ad-hoc network executing the DSR protocol, each packet contains the complete list of nodes that it has to traverse in order to reach the destination.

This feature, although excludes intermediate nodes form making any routing decisions, can still be exploited to create a wormhole. However, all such settings are primarily derived from scenarios where the colluding nodes (M1, M2) are not the immediate neighbors of the source (S) and destination (D) nodes, as shown in Fig 2.

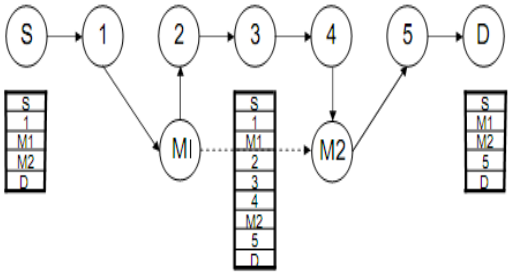

Fig. 2- Wormhole Creation in DSR

This feature, although excludes intermediate nodes form making any routing decisions, can still be exploited to create a wormhole. However, all such settings are primarily derived from scenarios where the colluding nodes (M1,M2) are not the immediate neighbors of the source (S) and destination (D) nodes, as shown in Fig (2).

Wormhole creation in such a scenario is generally accomplished using the following steps:

Sustained Routes between Colluding Nodes

M1 and M2 periodically establish and maintain routes to each other in the network at all times. This route serves as a higher layer tunnel for all other nodes whose traffic is routed through M1 and M2.

Fallacious Response to Source Node Route Requests

Whenever a ROUTE REQUEST packet from S is received by M1, it immediately sends a ROUTE REPLY packet so as to portray minimal delay. M1 also makes the ROUTE REPLY packet (S-1-M1-M2-D) as short as possible, indicating D as an immediate neighbor of M2.

Route Development till the Destination Node

M1 informs M2 to initiate a route discovery to D through a pre agreed upon higher layer protocol and also performs the same. In the mean time, all data packets from S to D are buffered for a certain interval at M1. While waiting for a route to D, if M1 receives a ROUTE REPLY packet from D to S, it verifies whether it can reach D through M2. If yes, it creates a new working source route option from M2 to D (S-M1-M2-5-D) for the buffered packets, encapsulates and sends them to M2, else it waits for the ROUTE REPLY packet to be received in response to the ROUTE REQUEST packet that was initiated by itself and M2. Upon receipt of these ROUTE REPLY packets, M1 traces an optimal route to D through M2.However, if during this waiting period, the buffer interval expires or an overflow occurs, M1 sends a ROUTE ERROR packet to S for the last received data packet.

Deception through Gratuitous Route Replies

As an alternate mechanism, if M1 overhears any ongoing communication between S and D (S-1-2-3-4-5-D). It may initiate a new route discovery to D and also request the same through M2. Upon receipt of a route from M1 to D via M2, it can create a new Gratuitous ROUTE REPLY packet (S-1-M1-M2-D) and send it to S. Based upon the same criterion for route selection, S may classify the newly received route as optimal and discard the one that was

already in use.

Translation of IP Addresses

IP Address translation is done both at M1 and M2 to successfully route all data through the created tunnel.

Trust Model

We detect and escape wormholes in the network using an effort-return based trust model. The trust model uses the inherent features of the Dynamic Source Routing (DSR) protocol to derive and compute respective trust levels in other nodes.

Each node executing the trust model, measures the accuracy and sincerity of the immediate neighboring nodes by monitoring their participation in the packet forwarding mechanism. The sending node verifies the different fields in the forwarded IP packet for requisite modifications through a sequence of integrity checks. If the integrity checks succeed, it confirms that the node has acted in a benevolent manner and so its direct trust counter is incremented. Similarly, if the integrity checks fail or the forwarding node does not transmit the packet at all, its corresponding direct trust measure is decremented. We represent the direct trust in a node y by node x as T and is given by the following equation:

$$T_{xy} = P_P . P_A$$

where $P_P \in [0, 1]$, represents the situational trust category Packet Precision, which essentially indicates the existence or absence of a wormhole through node y. P_A represents the situational trust category Packet Acknowledgements that preserves a count of the number of packets that have been forwarded by a node. The category P_P and P_A are employed in combination to protect the DSR protocol against wormhole attacks and for identifying selfish node behavior respectively. Any benevolent node not able to forward a data packet, due to radio interference, hardware faults, software bugs or environmental conditions, is classified as selfish. However, in case no other alternate trusted nodes are available, these selfish nodes will be engaged into the routing process. However, any node incorrectly forwarding a data packet, by not ensuring its integrity, will be classified as malicious and not included in any subsequent data connections.

Wormhole Detection

During wormhole detection, each node in the network measures the accuracy and sincerity of its immediate neighboring nodes. The detection process works in the following manner:

- Each node, before transmission of a data packet, buffers the DSR Source Route header. After transmitting the packet, the node places its wireless interface into the promiscuous mode for the Trust Update Interval (TUI). The TUI fundamentally represents the time a sending node must wait after transmitting a packet until the time it overhears the retransmission by its neighbor. This interval is critically related to the mobility and traffic of the network and needs to be set accordingly. If this interval is made too small it may result in ignoring of the retransmissions, similarly a large value may induce errors due to nodes moving out of range.
- If during the TUI, the node is able to overhear its immediate node retransmit the same packet, the sending node increases the situational trust category P_A for that neighbor. It then verifies whether the retransmitted packet's DSR Source Route header is the same as the one that was buffered earlier. If this integrity check passes, the situational trust category P_P is not set, indicating an absence of a wormhole. However, if the retransmitting node, modifies the DSR Source Route header, the detecting node sets P_P to true.
- In case no retransmission is heard and a timeout occurs when the TUI has exceeded, the situational trust category P_A for that neighbor is reduced and the DSR Source Route buffer is cleared.
- With the passage of time, the number of inter-node interactions also increase, increasing each node's knowledge of the behavior of other nodes. Any forwarding node, which had earlier detected wormhole creation by any of its immediate neighbor, drops all packets that were destined to go through that neighbor and generates a corresponding ROUTE ERROR packet. This packet informs the source and all intermediate nodes regarding the unavailability of the route through the wormhole. Consequently, the wormhole is circumvented in subsequent data connections.

Wormhole Escaping

In DSR, before initiating a new route discovery, the cache is first scanned for a working route to the destination. In the event of unavailability of a route from the cache, the ROUTE REQUEST packet is propagated. When the search is made for a route in the cache, the Dijkstra's algorithm [7] is executed, which returns the shortest path in terms of number of hops. In the LINK CACHE scheme the default cost of each link is one, which signifies uniform spread of the inter-node trust levels. So replace this cost with the actual trust level of a node to which this particular link is directed. Now, each time a new route is required, a modified variant of the search algorithm is executed, which finds routes with the maximum trust level. However, before cost assignment to any link, each node first checks the wormhole status of the link end node. If it has been classified as a wormhole, the cost of that link is set to infinity. This method ensures that wormholes nodes are avoided in all future data connections.

Conclusion

A wormhole is one such prominent attack that is formed by malicious colluding nodes. The detection and evasion of such wormholes in an ad-hoc network is still considered a challenging task. In order to protect from wormholes, current security-based solutions propose the establishment of ad-hoc networks in a controlled manner, often requiring specialized node hardware to facilitate deployment of cryptographic mechanisms. Such solutions, although successful in achieving self organization during the operation, essentially violate the self organized nature of an ad-hoc network. In this paper, it is deviated from the customary approach of using cryptography and instead employs a trust-based scheme to detect and escape wormholes. Moreover, it derives trust levels in neighboring nodes based upon their sincerity in execution of the routing protocol. This derived trust is then used to influence the routing decisions, which in turn guide a node to avoid communication through the wormholes.

References

[1] Pirzada A.A. and McDonald C. (2004) *Advanced Wired and*

Wireless Networks, 57-80.
[2] Dahill B., Levine B.N., Royer E. and Shields C. (2002) *Proceedings of the International Conference on Network Protocols (ICNP)*, 78-87.
[3] Johnson D.B., Maltz D.A. and Hu Y. (2003) *IETF MANET, Internet Draft (work in progress)*.
[4] Johnson D.B. and Maltz D.A. (1996) *Mobile Computing,* 353, 153-181.
[5] Maltz D.A., Johnson D.B. and Hu Y. (2007) *The Internet Engineering Task Force, Network Working Group*, *http:// www.ietf.org/rfc/rfc4728.txt*.
[6] Royer E.M. and Toh C.K. (1999) *IEEE Personal Communications Magazine*, 6(2), 46-55.
[7] Dijkstra E.W. (1959) N*umerische Mathematik,* 1, 269-271.
[8] Khalil I., Bagchi S. and Shroff N.B. (2005) *Dependable Systems and Networks* (*DSN*), 612-621.
[9] Khalil I., Bagchi S. and Shroff N.B. (2006) *Securecomm and Workshops,* 1-12.
[10] Hu L. and Evans D. (2004) *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 131-141.
[11] Capkun S., Butty´an L. and Hubaux J.P. (2003) *ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN),* 21-32.
[12] Wang W. and Bhargava B. (2004) *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, 51-60.
[13] Hu Y.C., Perrig A. and Johnson D.B. (2003) *Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*, 3, 1976-1986.
[14] Hu Y.C., Perrig A. and Johnson D.B. (2002) *Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (Mobi. Com.)*, 12-23.