Int. J. Advanced Networking and Applications
Volume: 03, Issue: 05, Pages: 1298-1301 (2012)

A Novel Wormhole Detection Technique for Wireless Ad Hoc Networks

Muhammad Sharif, Aisha Azeem, Mudassar Raza Waqas Haider
Email: muhammadsharifmalik@yahoo.com, aishaazeem19@gmail.com,
mudassarkazmi@yahoo.com, waqasbtn@gmail.com
Department of Computer Science, COMSATS Institute of Information Technology, Wah Cantt Pakistan

----------ABSTRACT----------
In this paper a wormhole detection technique has been proposed which makes use of AODV as an on demand routing protocol and secure neighbor detection protocol with certain modifications. In the technique, sender floods the route request packets in search of destination and in return the receiver responds by sending the route reply. The route reply contains the number of routes that lead to it, sending and receiving time, the identification of intermediate nodes and the request that the sender had sent. During analyzing the reply, sender confirms the number of routes by sending packets of verification to individual nodes whose identification has been stated by the receiver and based upon the delay in time i.e., Δt, wormhole link is detected. Analysis proves that the proposed technique not only detects the wormhole link but also provides a verification mechanism to judge the validity of nodes.

Key Words: Wormhole, Ad Hoc Networks, Intrusion, Packets

Date of Submission: October 03, 2011 Date of Acceptance: January 10, 2012

1. Introduction

In wireless ad hoc network communication links between the nodes are wireless and each node acts as a router for the other node, that is each node is willing to forward data to others. Such kinds of networks help in solving challenges and problems that may arise in every day communication [1]. On the other hand, Mobile Ad Hoc Networks (MANET) is a new field of research and is particularly useful in situations where infrastructure is costly e.g., emergency rescue operations, military deployments, oil drilling operations etc, however security of such networks is of great importance [2].

Although wireless network is more flexible but it is more subject to attacks due to its decentralized nature and vulnerabilities as compared to wired network which has a more rigid structure. The reason why wireless networks are subject to so many attacks is because it is decentralized, having limited resources [2] and scalable in nature. Due to decentralized nature of wireless networks, network intrusion is relatively easy. There are many security attacks that are faced by wireless ad hoc networks which are black hole attack, wormhole attack, rushing attack, message bombing, denial of services (DOS)/DDOS etc [3, 4, 5]. On the other hand, countering these attacks there is signature based intrusion detection in which a prewritten rule is used to detect an attack , another category includes anomaly based intrusion detection in which any abnormal activity that is detected and which deviates from normal profile is considered as anomaly and last but not least specification based intrusion as explained in [6,7, 8,9,10,11 ,12].

Wormhole is actually a severe attack on a MANET in which attacker drops packets randomly and establishes a fake link between two genuine nodes which are not within transmission range. In this paper the main emphasis is laid on wormhole attack and a solution to detect such an attack is proposed. The rest of the paper is organized as follows: Section 2 reviews the existing approaches to detect wormhole attacks, Section 3 exposes the proposed work and finally in Section 4 the concluded remarks are given.

2. Existing approaches to detect wormhole attack

Various techniques have been proposed to detect the wormhole attack. These techniques include packet leashing [4] i.e., packet leashing is inserted into each packet and on its basis expiration time of packet is determined. The other is the geographical leash which uses position of sender and sending time to determine the distance between them.

Another technique used for wormhole detection is directional antennas [13] in which specific sectors are used by the nodes to communicate with each other. So a neighbor communicating with the other node has some prior knowledge of its location.

In [14] wormhole attack is detected using an approach to exploit forbidden topology in the delay tolerant network. In the approach the transmission rage of the node is reduced during short period of time at the time of detecting wormhole link. In [15] the wormhole link is detected using exchange of encrypted packets among the neighbors, the technique verifies neighbors using 4-way handshaking message exchanging among two supposed neighbors. In [16] as an application of wormhole, the anti -jamming techniques have been proposed in wireless sensor networks. After analyzing these techniques a novel wormhole detection technique is presented which not only provides a secure path to destination but also authenticates the intermediate nodes.

3. Proposed Technique

As mentioned in AODV [17] protocol the sender first floods the *ROUTE REQUEST* packets to establish the path to the destination by inserting sending time and its ID. Once the

Volume: 03, Issue: 05, Pages: 1298-1301 (2012)

request message reaches at the receiver end, the receiver responds with its ID, number of routes, receiving time and ID's of intermediate nodes (if any) which helped in passing the request to destination. The sender then retrieves the information sent by receiver, sends packets of verification to intermediate nodes to see their legality of being neighbors and also verifies the data. Delay in time determines the wormhole link.

3.1 System Model and demonstration

From Figure 1 following assumptions can be made:

- A,B,C,D,F are communicating nodes
- Sender node A and destination node F
- To reach F there are two paths:
  - A,B,C,D,F
  - AXF
- where X is the intruder node

Following are the major steps for exploring proposed technique working.

3.1.1 Initializing and Requesting. In Figure 1, suppose node A wants communication with node F, then node A broadcasts route request packets. This broadcast is also received by the wormhole which forwards the request to the next node. The request also travels in the network in the appropriate way i.e., via valid nodes. This makes node F thinks that there are two paths to node A; a 4-hop path through B, C and D and a single hop direct link. Routing protocols would obviously prefer the shorter route, hence giving preference to the wormhole. When route request reaches at the destination, the receiving node responds with a ROUTE REPLY with its receiving time (e.g., Tr), the number of routes that lead to it and the identification of intermediate nodes which helped in passing the request to F. The sender then retrieves the receiving time, number of routes and ID's of each node.

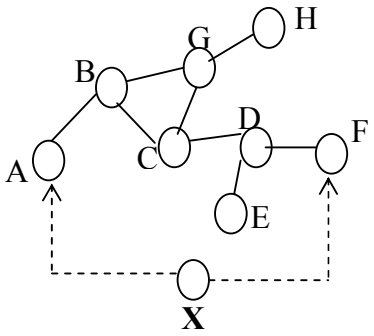

Figure 1: Various communicating nodes having an intruder node X represented by dotted line

3.1.2 Validation of Nodes. Getting full acknowledgement that the given nodes are in-fact true neighbors, the legality of A-F direct link is also inspected. Since most of on-demand routing protocols unconditionally perform neighbor detection, hence each node receiving the ROUTE REQUEST assumes to be its neighbor but this assumption does not prevent the intruder from getting the request. To avoid this secure neighbor detection protocol [5] can be used.

In order to verify that the nodes are valid, sender sends packets of verification to authenticate those nodes. It sends a request, encrypts nonce N1, sending time Ts and ID's that F had sent using its encrypted key. This process can be depicted as follows:

A→ B: verify [Request || ID_B || Ts || E_A (N1 || ID_A)]
B →A: verify [Request || ID_A || Tr || E_B (N2 || ID_B)]
A→ B: verify [E_B (N2 || ID_B]

B replies A with the same request, receiving time Tr and applied a function on the nonce to verify that it is the same request sent by A. The delay between sending the request and receiving the reply is ΔT. If ΔT is sufficiently small then A-B are within transmission range. Same process is applied to all the nodes whose identification is provided by F.

Now to analyze the A-F direct link, above mentioned process is applied to node F but this time no ID of intermediate nodes is mentioned because F didn't reply any ID's that came across in second route and mentioned it as a direct link i.e.,

A→ F: verify [Request || ID_F || Ts || E_A (N1 || ID_A)]
F →A: verify [Request || ID_A || Tr || E_F (N2 || ID_F)]
A→ F: verify [E_F (N2 || ID_F]

Delay is calculated as mentioned above but if ΔT is larger than the one calculated for A-B link whose ID was provided by node F in its ROUTE REPLY as the first node to receive the broadcast of ROUTE REQUEST, then it means sender and receiver are not within transmission range but are connected by some fake link i.e., wormhole link that makes both nodes think that they are within transmission range, so this route is discarded. Once wormhole is detected, valid route is followed to carry out the remaining communication process.

3.1.3 Communication processes with notations and examples. Steps of the communication process with notations are:

Route request packets

A sends [Request || IDa || Ts || IDf]
F reply [Request || IDa || Ts || Tr || IDf || ID of intermediate nodes || no of paths]

Sender retrieves information from reply

Request, IDa, Ts, Tr, IDf , ID's of B,C,D
Number of paths i.e,

- A.B,C,D,F
- A,**X**,F

Verification of nodes and paths

Sender now sends verification packets to intermediate nodes individually i.e,

A→ B: verify [Request || ID_B || Ts || E_A (N1 || ID_A)]
B →A: verify [Request || ID_A || Tr || E_B (N2 || ID_B)]
A→ B: verify [E_B (N2 || ID_B]
ΔT_{AB}= Tr-Ts is calculated

A→ C: verify [Request || ID_C || Ts || E_A (N1 || ID_A)]
C →A: verify [Request || ID_A || Tr || E_C (N2 || ID_C)]
A→C: verify [E_C (N2||ID_C]
ΔT_{AC}= Tr-Ts is calculated

A→ D: verify [Request || ID_D || Ts || E_A (N1 || ID_A)]
D →A: verify [Request || ID_A || Tr || E_D (N2 || ID_D)]
A→ D: verify [E_D (N2 || ID_D]

Volume: 03, Issue: 05, Pages: 1298-1301 (2012)

Again ΔT_{AD} is calculated

Now to verify the second path i.e., A-F direct link
A→ F: verify [Request || ID_F || Ts || E_A (N1 || ID_A)]
F →A: verify [Request || ID_A || Tr || E_F (N2 || ID_F)]
A→ F: verify [E_F (N2 || ID_F]
ΔT_{AF}=Tr-Ts is calculated

If $\Delta T_{AF} > \Delta T_{AB}$ i.e., if ΔT_{AF} is larger than the one calculated for A-B link whose ID was provided by node F in its ROUTE REPLY as the first node to receive the broadcast of ROUTE REQUEST, then it means sender and receiver are not within transmission range but are connected by some fake link i.e., wormhole link and hence this link is discarded.

Example for verification phase
For A to communicate with C, D and F during verification, it will take following amount of time:

A->C =$\Delta T_{AB} + \Delta T_{BC}$ = 2+2=4 msec
A->D =$\Delta T_{AB} + \Delta T_{BC} + \Delta T_{CD}$ = 2+2+2=6 msec
A->F =$\Delta T_{AB} + \Delta T_{BC} + \Delta T_{CD} + \Delta T_{DF}$ = 2+2+2+2= msec

This implies that $\Delta T_{AF} > \Delta T_{AB}$. From this supposition it can be seen that it takes six times more longer to send and receive the message to node F. This proves that A and F can't be directly connected but are attached to some fake link which makes them believe that they are direct neighbors. Also it can be seen that the node that is direct neighbor of A is node B and it only takes 2 milliseconds for both of them to communicate with each other.

Example Having Multiple Paths to Destination Node
In this section same process will be applied to detect the wormhole link but this time there are multiple paths from source to destination. In this case best path will be selected on the basis of average time that takes to reach destination. Following scenario illustrates this process:

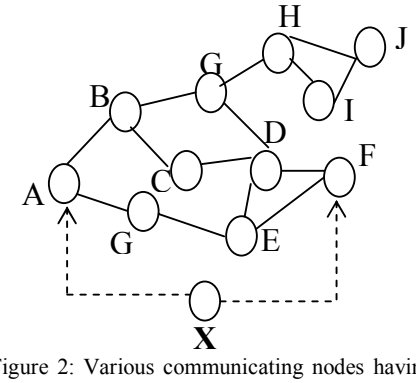

Figure 2: Various communicating nodes having multiple paths to reach destination node F.

From figure 2 the intruder node can be detected by calculating the average time to reach the destination node and this time can be compared with any of the nodes that directly connect the sender node. Assuming it takes 2 milliseconds for each neighbor to communicate, Table 1 represents the possible routes that can be followed and the time it takes and finally average of all these routes is calculated to determine the approximate time it takes to reach destination node.

No. of Routes	Sender Node	Intermediate nodes	Receiver node	Time taken
1	A	GE	F	6msec
2	A	GED	F	8msec
3	A	BCD	F	8msec
4	A	BCDE	F	10msec
5	A	BGD	F	8msec
6	A	BGDE	F	10msec

Table1 showing possible routes and the time taken to reach destination node

From all these the average time is calculated as follows:

$$\Delta \mathbf{T_{AVG}} = \sum_{\mathbf{p=1}}^{\mathbf{N}} (\Delta \mathbf{T_{Total\ Routes}}) / \mathbf{N} \quad \text{.....(1)}$$

where ΔT_{AVG} is the average time , p represents number of paths which go up to n.

Putting values in equation 1

$$\Delta T_{AVG} = \sum_{p=1}^{6} (6+8+8+10+8+10)/ 6$$

$\Delta T_{AVG} \approx 8$ msec

From this calculation it can be clearly seen that it takes approximately 8 milliseconds for A and F to communicate and there is no way A and F are directly linked. As seen from figure 2, A's direct neighbors are B and G and it takes 2 msec to communicate with them. From both scenarios it can be seen that whether there is single route or multiple routes to destination, in both cases intruder node can be detected by determining the time it takes to reach destination node.

4. CONCLUSION

In this paper wormhole detection technique has been proposed that provides a secure and authenticated path for nodes to communicate and clearly detects the fake link provided by the wormhole. The periodic exchange of information among the neighbors validates the ad hoc network reliability. Another plus point of this technique is that it uses a verification mechanism to judge the validity of nodes. Therefore, the proposed technique is capable of ensuring ad hoc network's security where wormhole attacks ratio is high.

5. References

[1]. Xia Wang, "Intrusion Detection Techniques in Wireless Ad Hoc Networks". COMPSAC '06. 30th Annual International Computer Software and Applications Conference, 2006, Volume: 2, On Page(S): 347-349.

[2]. Yongguang Zhang, Wenke Lee, Yi-An Huang, "Intrusion Detection Techniques For Mobile Wireless Networks". Wireless Networks, V.9 N.5, P.545-556, September 2003.

[3]. Nagrath, Preeti; Gupta, Bhawna." Wormhole Attacks in Wireless Adhoc Networks and their Counter Measurements: A Survey". 3rd International Conference on Electronics Computer Technology (ICECT), 2011. Page(S): 245 – 250

[4]. Y.-C. Hu, A. Perrig, and D.B. Johnson, "Wormhole Attacks In Wireless Networks," *IEEE J. Selected Areas In Comm.,* Vol. 24, No. 2, Feb. 2006, Pp. 370–380.

[5]. Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Rushing Attacks And Defense In Wireless Ad Hoc Network Routing Protocol". Workshop On Wireless Security Proceedings Of The 2nd Acm Workshop On Wireless Security San Diego, Ca, Usa, 2006.

[6]. Yang H, Luo H, Ye F, Lu S, Zhang L. "Security In Mobile Ad Hoc Networks: Challenges And Solutions". *IEEE Wireless Communication* 2004; Pages: 38-47.

[7]. C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, And K. Levitt, "A Specification-Based Intrusion Detection System For Aodv," In The 1st ACM Workshop On Security Of Ad Hoc And Sensor Networks, Conference On Computer And Communications Security, 2003, Pp. 125-134.

[8]. Das, Abhijit; Basu, Soumya Sankar; Chaudhuri, Atal." A Novel Security Scheme for Wireless Adhoc Network". 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011. Page(S): 1 – 4.

[9]. Singh, U.; Reddy, B.V.R.; Hoda, M.N." GNDA: Detecting Good Neighbor Nodes in Adhoc Routing Protocol". Second International Conference on Emerging Applications of Information Technology (EAIT), 2011. Page(S): 235 – 238.

[10]. Jian Ren; Yun Li; Tongtong Li. "Providing Source Privacy in Mobile Ad Hoc Networks". IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, 2009. Page(S): 332 – 341.

[11]. Esfandi, A." Efficient Anomaly Intrusion Detection System in Adhoc Networks by Mobile Agents". 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010. Page(S): 73 – 77.

[12]. Prathapani, A.; Santhanam, L.; Agrawal, D.P."Intelligent Honeypot Agent for Blackhole Attack Detection in Wireless Mesh Networks". 6th International Conference on Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE. Page(S): 753 – 758.

[13]. Hu and D. Evans. "Using Directional Antennas to Prevent Wormhole Attacks". Network and Distributed System Security Symposium, San Diego, 5-6 February 2004.

[14]. Yanzhi Ren; Mooi Choo Chuah; Jie Yang; Yingying Chen." Detecting Wormhole Attacks in Delay-Tolerant Networks [Security and Privacy in Emerging Wireless Networks]". Ieee Journal on Wireless Communications. 2010 , Page(S): 36 – 42

[15]. Nait-Abdesselam, F." Detecting and Avoiding Wormhole Attacks In Wireless Ad Hoc Networks". Ieee Communications Magazine, Publication Year: 2008, Page(S): 127 – 133.

[16]. Cagalj, M.; Capkun, S.; Hubaux, J.-P." Wormhole-Based Antijamming Techniques in Sensor Networks". IEEE Transactions on Mobile Computing. Publication Year: 2007 , Page(S): 100 – 114

[17]. C.E Parkins And E. M Royer, " Ad-Hoc On-Demand Distance Vector Routing", Sun Microsystems Labs, Menlo Park , CA 94025, USA And University Of California, Santa Barbara, CA , USA.1999