An Statistical Technique to Mitigate Black Hole Attack in Wireless Network

K.Mahamuni,
Research Scholar,
Department of Computer Science,
Periyar University,
Salem-11, TamilNadu, India.

C.Chandrasekar, PhD.
Associate Professor,
Department of Computer Science,
Periyar University,
Salem-11, TamilNadu, India.

ABSTRACT

Network nodes function as routers in ad hoc networks forwarding data packets that had its genesis in other nodes for communication extending beyond transmission range. Usually, ad hoc network routing protocols are built to function well in non-adversarial surroundings. Routing protocol security is critical in settings where networks face attacks which disrupt communication. This paper proposes to simulate/study black hole attack impact in ad hoc networks with DSR routing protocol. The obtained output is the basis for a novel statistical method to identify black hole attack based on RREQ control packet sequence. The proposed method is able to identify black hole attacks in the network and avoid the node during new route discovery.

KEYWORDS

Adhoc network; network security; network attacks; Dynamic Source Routing (DSR);

1. INTRODUCTION

In certain situations, it is necessary to have a temporary network without any physical infrastructure or centralized administration. This temporary network is made possible by a collection of wireless hosts – which are called ad hoc networks. In ad hoc networks, network nodes function as routers and relay data packets originated from other nodes to communicate beyond transmission range. Applications of ad hoc network such as military exercises, disaster relief not only requires reliable but also secure communication. Some of the features that have to be kept in mind when security is considered are: availability, confidentiality, integrity, authentication, and non-repudiation [1].

Ad hoc network's wireless links have many problems, making them susceptible to attacks like message distortion and impersonation i.e, an unknown person can access private data, modify and even delete it. Because these networks are temporary they can be attacked from within, due to being constructed without protection, in poor conditions. Attacks are also launched if nodes are compromised. Another issue is the node number. Hundreds/thousands of nodes might be required in a network and security measures undertaken must be efficient and cost-effective for a vast network. Exchange of topological information among nodes is facilitated by routing protocols to establish routes and this is used by attackers for acts including bogus routing, incorrect forwarding, lack of error messages, restricted reply time, thereby leading to retransmission and inefficient routing [2].

Dynamic Source Routing (DSR) is developed for ad hoc network routing [3, 4]. DSR is a source routing protocol where a source node specifies the route that the packet should use. Basic DSR mechanisms include Route discovery and Route maintenance. Neighbor nodes get a ROUTE REQUEST(RREQ) message from nodes to establish a route. On receipt of this message it is forwarded to neighbors by nodes and put themselves into the source route. On receipt of the message by destination node or a node having route information to the destination in its route cache, the node sends a reply containing information about the full source route. Then the source node picks up shortest route and stores it, and forwards messages along it. Routes with better route metrics get priority and this is in the cache for a longer duration. Usually, the route metrics considered include are the hop number, delay, bandwidth and the duration for the ROUTE REPLY(RREP) to reach the source. Route maintenance is activated when a break on the route is detected by the source node while forwarding data packet to a destination. When a link from node itself and to the next node is broken, it sends a ROUTE ERROR(RERR) message to the source node, which while removing the broken link from its route cache, uses another route to the destination. If another route is not available, it starts a route discovery again.

Routing disruption attacks and resource consumption attacks are both routing protocol attacks [5]. They are observed by through monitoring each node's component event and are detected immediately or when they occur repeatedly. Some methods to detect attacks include:

- Incorrect forwarding detection through passive acknowledgment.
- Bogus routing identification when intermediate nodes do not have same route information in its cache even after advertising.
- Indicating salvage through the absence of link error message before receipt of a salvaged message.
- Restricted reply time detection by comparing it to actual route length.
- Detection of bogus route metrics by comparing metrics to actual quality

Common attacks faced by networks include blackhole, grey hole and wormhole attacks and IP spoofing. Blackhole attacks are malicious nodes that refuse to forward traffic. A malicious node claims to have a shortest route to a destination leading to all traffic being forwarded to it. Black hole nodes are invisible and can be detected by monitoring lost traffic. Similar to a black hole attack, a Greyhole attack is when only data packets are not forwarded. A Wormhole attack takes place when a malicious node recording packets in one location sends them to another through a tunnel. In conflict-detection allocation, a new node chooses a random address and broadcasts a conflict detection packet throughout the MANET. A node veto prevents it from using this address. When a malicious node repeatedly impersonates a member occupying the same IP address and replies with vetoes repeatedly, it is known as an IP Spoofing attack. This paper proposes a study of black hole attacks in DSR aided network. Statistical techniques study the correlation between past control packet overheads and present overheads.

2. LITERATURE REVIEW

Literature has many innovative methods [6, 7, 8] to ensure security for an ad hoc network. A suggestion is that there is a distinction between a network with an a priori trust relationship between nodes and one which lacks trust between nodes. Another suggestion is to secure key management service in a networking environment to ensure secure routing as these two issues are very important and essential. Failures are tolerated through use of redundancies in network topology and by utilizing diversity coding. Seung Yi et al. [9] suggested a new technique known as “Security-Aware ad hoc Routing” (SAR) where security features are included as parameters in route discovery process.

Hu et al., [10] presented ‘Ariadne’ a DSR based protocol for route protection which could be used with several authentication mechanisms like digital signatures, MACs computed with pair-wise secret keys, or TESLA. Compromised node attacks which tamper with uncompromised nodes/denial of service attacks can be prevented by the new procedure. Every route request should be authenticated using hash chain elements to protect a network from being overloaded with counterfeit route requests. Discovered paths can be protected by combining TESLA authenticators (MACs) added by intermediate routers and hash technique. The proposed method's security mechanisms are very efficient and useful for a various routing protocols.

Nodes being categorized on a dynamic measured behavior was suggested by Marti et al. [11]. The proposed method increased throughput in MANETs through complementing DSR with a watchdog and path rater. While a watchdog detected malicious behavior, the pathrater rated trust management and routing policy on a paths, thereby ensuring that nodes avoided malicious nodes on routes to deliver data packets. Simulation proved the efficient performance of the proposed method, increasing throughput by 17% when 40% misbehaving nodes were present.

All literature revealed techniques are reactive with not even one learning from past data regarding mitigating attacks. This paper proposes to locate a correlation between past history and current pattern for Black hole attacks identification.

3. PROPOSED METHODOLOGY

A generally used statistical technique is Correlation providing the relationship degree between two variables. The correlation value provides a statistical similarity between two variables, from total correlation to no correlation with values ranging from 1 to 0. A correlation analysis provides better data understanding. Correlation quantifies data but not categorical data. Correlation is represented by correlation coefficient, generally ranging from -1 to +1. A correlation is positive when its coefficient is nearer +1 and negative when value is closer to -1. Correlation calculation is as follows:

$$r = \frac{N\sum xy - \left(\sum x\right)\left(\sum y\right)}{\sqrt{\left[N\sum x^2 - \left(\sum x\right)^2\right]\left[N\sum y^2 - \left(\sum y\right)^2\right]}}$$

Where: N = number of pairs of score (x, y)

$\sum xy$ = sum of the products of paired scores

$\sum x$ = sum of x scores

$\sum y$ = sum of y scores

$\sum x^2$ = sum of squared x scores

$\sum y^2$ =sum of squared y scores

This paper proposes study of correlation between historical data with nil attacks, monitoring the same in control packets. The proposed analysis uses Route Request (RREQ) control packets to detect if any are positively or negative correlated. When correlation is negative on comparison with historical data under similar network conditions, it is assumed to be an attack.

4. EXPERIMENTAL SETUP

The experimental setup consists of over 20 nodes spread over an area of 500 m x 500 m in OPNET Simulator. The nodes are moving randomly. Each node has a transmission power of 0.0005 w and data rate of 11 Mbps. DSR routing protocol parameters were set as shown in table 1.

TABLE 1. DSR ROUTING PARAMETERS USED

Route expiry time	300 second
Request table size	64
Maximum transmission attempt	16
Timeout value for non-propagating requests	0.03 second
Gratuitous route reply timer	1second
Maintenance hold off time during route maintenance	0.25 second
Maintenance acknowledgement time	0.5 second

Two scenarios are considered, in the first scenario contains three malicious nodes utilize a high power transmitter and receiver for black hole attack as shown in Figure 1. The second scenario is made of a normal network without attack which is based on historical data. Experimental results obtained are shown in the next section.

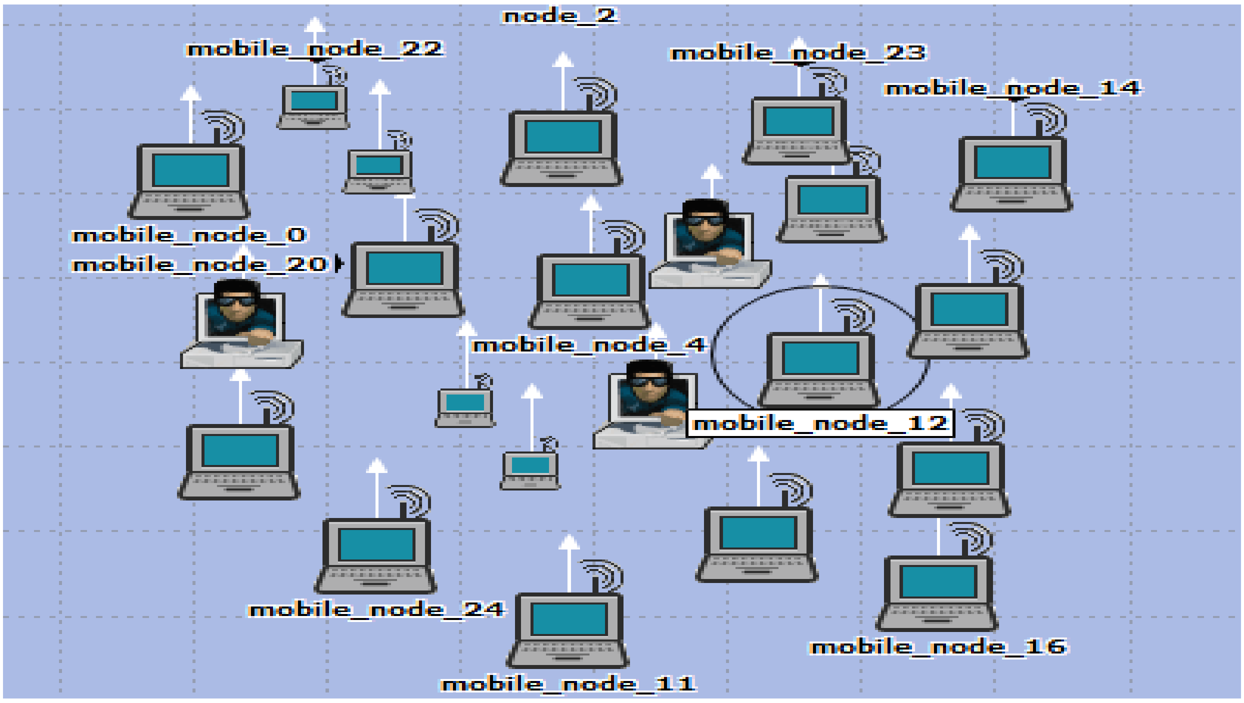

Figure 1. The experimental setup with three malicious nodes

5. RESULTS AND DISCUSSIONS

Simulation of the proposed architecture was carried out for 300 seconds and the results obtained are tabulated in figure 2 to figure 6.

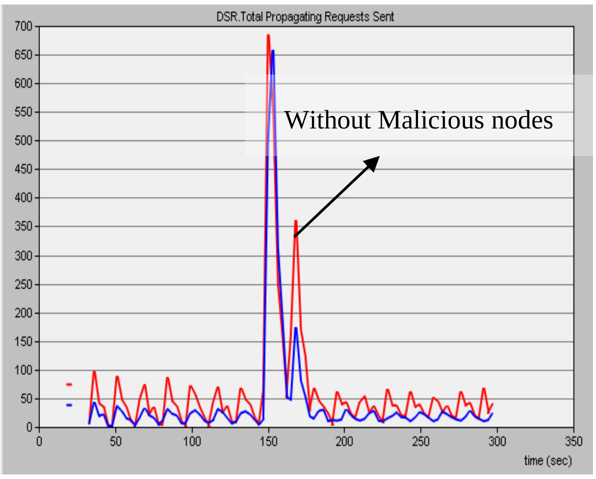

Figure 2. Total propagation results sent

It can be seen with the presence of malicious nodes, the broadcast of requests is affected and decreases by almost 50% which can decrease the QOS(see figure 2).

Though the route discovery time is not affected due to the RREP sent back by the malicious nodes (as shown in Figure 3).

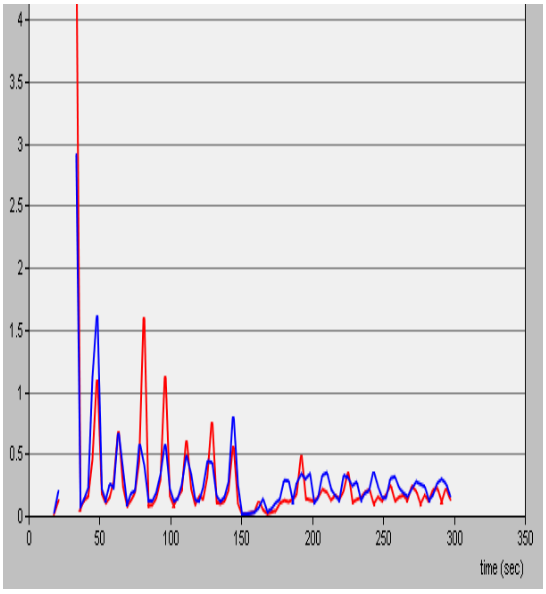

Figure 3. Route discovery time

The route request and replies sent between source and destination also decreases due to the drops caused by the malicious nodes as shown in Figure 4 and Figure 5. Since route discovery is affected it can be seen the performance of the network degrades proportionately.

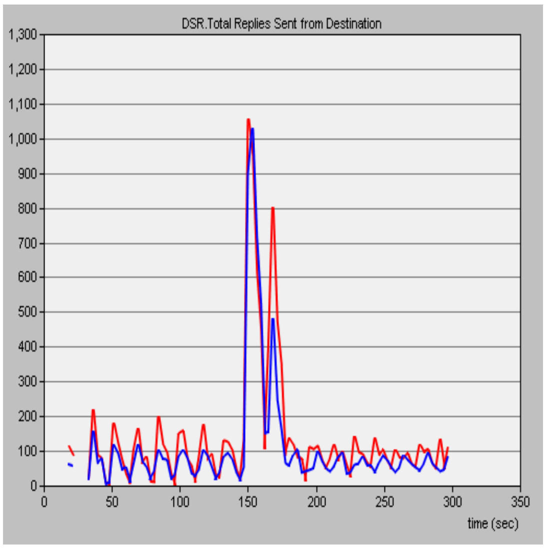

Figure 4. Replies received from destination

From figure 5, it can be seen an attack is present in the network as the correlation between the data is high. The network shows an ongoing attack.

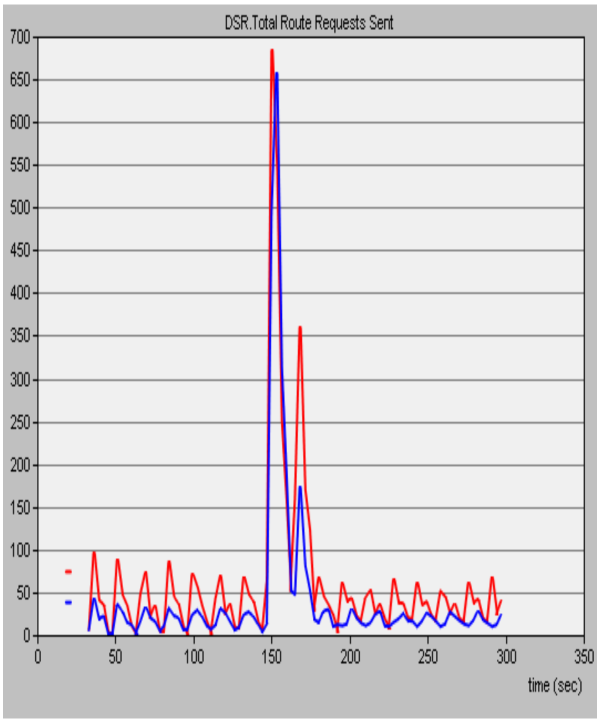

Figure 5. Correlation graph of the Route requests sent between historical and current data

Figure 6 shows the throughput of the system. It can be seen that due to inconsistent route discovery and packet dropping by the malicious nodes, the throughput drops by more than 30%.

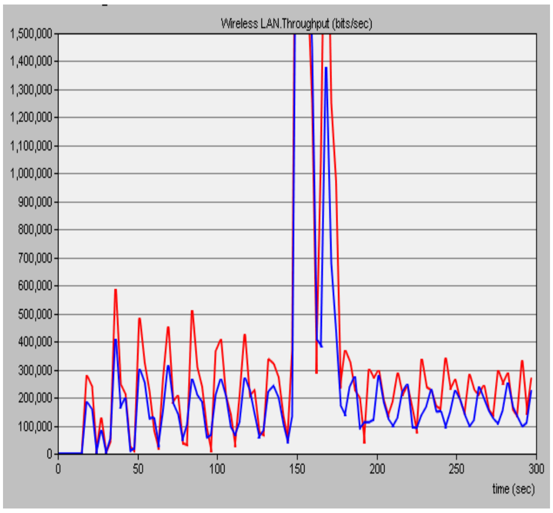

Figure 6. The throughput of the system

6. CONCLUSION

This paper proposes prediction of black hole attacks in DSR enabled wireless networks. To evaluate the proposed method, a simulation set up including 15% network nodes acting as malicious nodes dropping packets received is used. Simulations were run for 300 seconds revealing that even with a small group of malicious nodes network degradation was more than 30% with respect to throughput. As Ad hoc networks are formed by co-operating individual nodes, identification of malicious nodes is of paramount importance to alleviate effects caused by it in avoiding security issues and network degradation. The proposed correlation based evaluation of two scenarios gives enough data to know whether a network is under attack or not.

7. REFERENCES

[1] Lidong Zhou, Zygmunt J. Haas, “Securing Ad Hoc Networks”, IEEE Network Magazine, Vol. 13, No. 6, Nov./Dec. 1999, pp. 24–30.

[2] S. Buchegger, J.-Y.L. Boudec, Nodes bearing grudges: towards routing security, fairness, and robustness in mobile ad hoc networks, in: Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing, IEEE Computer Society, Canary Islands, Spain, 2002, pp. 403–410.

[3] D. B. Johnson and D. A. Maltz. The dynamic source routing protocol for mobile ad hoc networks. Internet Draft, Mobile Ad Hoc Network (MANET) Working Group, IETF, October 1999.

[4] David B. Johnson. Routing in Ad Hoc Networks of Mobile Hosts. In Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications (WMCSA’94), December 1994, pp. 158–163.

[5] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. Technical Report TR01-384, Department of Computer Science, Rice University, June 2002.

[6] Ralf Hauser, Antoni Przygienda, and Gene Tsudik. Reducing the Cost of Security in Link State Routing. In Symposium on Network and Distributed Systems Security (NDSS '97), February 1997, pp. 93–99.

[7] Andy Heffernan. Protection of BGP Sessions via the TCP MD5 Signature Option. RFC 2385, August 1998.

[8] Adrian Perrig, Ran Canetti, Dawn Song, and J. D. Tygar. Efficient and Secure Source Authentication for Multicast. In Network and Distributed System Security Symposium, NDSS '01, February 2001, pp. 35–46.

[9] Seung Yi , Prasad Naldurg , Robin Kravets, "Security-aware ad hoc routing for wireless networks," Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing, October 04-05, 2001, Long Beach, CA, USA.

[10] Y.-C. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking, Atlanta, GA, Sept. 2002.

[11] S. Marti, T. Giuli, K. Lai, and M. Baker. "Mitigating routing misbehavior in mobile ad hoc networks." In Proceedings of MOBICOM' 2000, 2000, pp. 255–265.

AUTHOR'S PROFILE

K. Mahamuni received the B.Sc.(Computer Science) degree from the Bharathidasan University Tiruchirappalli, in 1992. He received his MCA and M.Phil(Computer Science) Degrees from Manonmaniam Sundaranar University, Tirunelveli, in 1995 and 2001, respectively. He is currently pursuing the Ph.D. degree with the Department of Computer Science, Periyar University, Salem, TamilNadu, India. His research interests include Mobile Computing and Wireless Networking.

Dr. C. Chandrasekar received his Ph.D., degree from Periyar university. He is working as an Associate Professor, Department of Computer Science, Periyar University, TamilNadu, Salem, India. His areas of interest include Wireless networking, Mobile Computing, Computer Communications and Networks. He is a research guide at various universities in India. He has published more than 80 technical papers at various National & International conferences and 50 journals.