Performance Evaluation of ABR Routing in Malicious Network

[1]K.Geetha [2]Dr.P.Thangaraj
[1]AP/IT,Excel engineering college,
Komarapalayam,India.
srirajgeetha@gmail.com
[2]HOD,CSE
Bannari Amman Institute of Technology, India

[3]C.Rajan [4]Dr.N.Shanthi
[3]Research Scholar [4]HOD,IT
K. S. Rangasamy College of Technology,India
rajancsg@gmail.com

Abstract— Mobile ad hoc networks (MANETs) include wireless communication and mobile nodes. High node mobility and limited wireless communication range mean that nodes have to cooperate in order to ensure networking, with the network changing to meet needs continually. Protocols' dynamic nature enables MANET operation to ensure deployment in extreme/volatile circumstances. Hence, MANETs are very popular research topics and have been used in areas like tactical operations, rescue operations and environmental monitoring. This paper proposes a method to mitigate malicious nodes forming Denial of service attacks in associativity based ad hoc network. It is divided into two phases: detection before route establishment and avoiding malicious nodes in data forwarding. Simplicity and effectively detecting malicious nodes are the main points of the proposed scheme.

Keywords- *ASSOCIATIVITY BASED ROUTING (ABR); Denial of service attacks (DOS).*

I. INTRODUCTION

Portable computing and wireless technology advances are opening up possibilities for mobile networking. MANET, the vision of the Internet Engineering Task Force (IETF) provides improved standardized routing functionality to support self-organizing mobile networks. Mobile ad hoc networking technology applications include industrial, commercial, and military communication networks which include cooperative mobile data exchange in places where wireless mobile nodes comprise communication infrastructures.

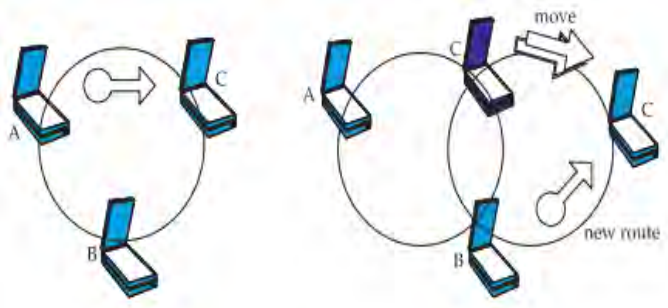

Figure1: ADHOC network

Mobile Ad Hoc Networking technology is being developed over the last two decades mainly through U.S. Government sponsored funding. Its first sponsors were Defense Advanced Research Projects Agency (DARPA), the U.S. Army and Force on Naval Research (ONR). Early packet radio programs included Survivable, Adaptive Networks (SURAN) Program, the Low-cost Packet Radio (LCR) Program and Survivable Communication Networks (SCN) Program [1]. Government-sponsored work is on in networking programs like Tactical Internet and Near Term Digital Radio (NTDR).

A MANET includes mobile platforms, moving freely and arbitrarily with platforms being called "nodes." It includes a router with many IP-addressable hosts and numerous wireless communications devices. A node may have separate networked devices or be integrated into one device like a laptop/handheld computer. Nodes have wireless transmitters/receivers with antennas which can include omnidirectional (broadcast), highly directional (point-to-point), steerable (arrays) or a combination of these. At a point in time, based on nodes' positions and

transmitter/receiver coverage patterns, transmission power levels, and co-channel interference, wireless connectivity exists between the nodes [2] as a dynamic, multi-hop graph or "ad hoc" network.

Ad-Hoc networks are dynamic, multi-hop wireless networks established by mobile nodes on shared wireless channels. Each mobile host broadcasts locally to identify its presence to surrounding hosts. The latter are nodes near the transmitting host. Thus, every mobile host is a potential router, establishing routes between self, and route possessing nodes. Ad-Hoc Networks were first meant for applications like battle field communications and disaster recovery, but Multimedia Technology evolution and company's commercial interest to reach civilian applications ensured that QoS in MANETs generated high interest [3].

These temporary networks can be attacked from within, due to their protection free construction in poor conditions. When nodes are compromised, attacks occur. Node number is another issue. As hundreds/thousands of nodes are in a network, security must be efficient and cost-effective. Nodes' topological information exchange is via routing protocols to establish routes which in turn are used by attackers for incorrect forwarding, bogus routing, restricted reply time and lack of error messages leading to retransmission/inefficient routing. Works which addressed MANET intrusion responses isolated uncooperative nodes based on node reputation through their behavior. This anti-malicious node response neglects negative side effects. Improper countermeasures in MANETs can lead to unexpected network partition which also increases network infrastructure damage. More flexible/adaptive responses need investigation when addressing such critical issues [4].

MANET attacks are classified into 2 categories; passive and active attacks. A passive attack obtains network exchanged data without disrupting communications, while active attacks involve information interruption, modification/fabrication, disrupting normal MANET functions. Examples of such attacks are traffic analysis, eavesdropping and traffic monitoring. Active attacks include impersonating, jamming, Denial of Service (DOS), modification, and message replay. Attacks can be classified into 2 categories; external and internal attacks based on attack domains [5].

ABR compromises broadcast and point-to-point routing maintaining routes for sources desiring routes. But it uses INS based alternate route information avoiding stale routes. Also, routing decisions are undertaken at DEST with the best route being selected/ used while other routes are passive thereby avoiding packet duplicates [6].

This paper proposes ABR based routing modified with a detection algorithm. It is split into 2 phases: Detection while establishing routes and Detection when forwarding data. The proposed scheme's silent feature is simplicity and effectiveness in malicious node detection even when the network is dynamic. The remainder of the paper is as follows: Section 2 deals with related works, Section 3 describes the methodology, Section 4 details results and section 5 concludes the paper.

II. LITERATURE SURVEY

A work dealing with ad hoc routing protocol classification was suggested by Kuosmanen (2002) [7] who also proposed specified protocols according to such classification. The protocols presented were based on an entity formed by the mentioned paper and related papers and was published by the HUT Networking Laboratory. The work emphasized a variety of protocols to evaluate their suitability/tradeoffs.

Sivavakeesar and Pavlou (2005) [8] presented a framework to dynamically organize mobile nodes (MNs) and elect a dominating set in spontaneous large-scale MANETs aimed at supporting location based routing protocols. This strategy was called sociativity-based clustering, where a node was chosen as the cluster head (CH). This was dependent on nodes' associativity states implying periods of spatial/temporal stability. The heuristic used in clustering ensured a dynamic, distributed/adaptive operation of the suggested protocol. Further, the heuristic considered node mobility as the main criterion in cluster head election leading to stable cluster formation. The CH election process heuristic ensured that responsibility of being a cluster head was distributed among nodes, and hence was fair. Simulation demonstrated this strategy's performance advantage.

New possible attacks on ad hoc networks like a black hole/cooperative black hole attacks were analyzed by Bhalaji, et al., (2011) [9]. In this, a malicious node advertises as having a shortest node path whose packets it plans to intercept. It waits/checks replies from neighboring nodes for a safe route location to reduce the probability. When such nodes work in groups, damage then is massive and is called a cooperative black hole attack. The solution is the location of a secure route between source and destination through identification/isolation of black hole nodes. The paper evaluated the proposed solution through simulation, comparing it to the standard DSR protocol as regards throughput, latency and packet delivery ratio.

AODV and DSR performances were investigated by Dadhania, et al., (2013) [10] both with / without black hole attacks (malicious node) through CBR traffic under various network mobility's. Evaluated effect simulation was

compared with standard protocols regarding Packet delivery ratio, throughput and End to End Delay. Experiments with network simulator-2 for 50 node ad hoc networks proved that AODV was more susceptible to Black Hole attack than DSR.

A stability and hop-count based approach to MANET routing was presented b Sridhar and Chan (2005) [11], where the stability metric is a link's residual life. The authors viewed stability based routing as an enhancement to hop-count based routing protocol (e.g. DSR or AODV), so that anticipated life and route hop count are considered. How residual link life was affected by parameters like speed/mobility pattern through simulation was first investigated. The result proved that residual link life is a current linkage, mobility speed and mobility pattern function not varying monotonically with age. Hence, intuitive ideas like older links being more stable, used in present stability-based routing algorithms like Associativity Based Routing (ABR), do not hold on a vast spectrum of mobility speed/models. Instead, the reverse is true. The authors proposed stability/hop-count based routing algorithm (SHARC) using DSR as routing protocol. Path stability was calculated with a histogram based estimator. Simulation revealed that SHARC performed better than hop-count along algorithm (DSR) and stability only algorithm for both throughout of long TCP and short data transfer response time. SHARC performs close to algorithm with link residual lifetime knowledge in many cases.

Murugan and Shanmugam (2010) [12] used 3 techniques simultaneously including a cumulative frequency based detection technique to detect MAC layer attacks, data forwarding behavior based technique to detect packet drops and message authentication code technique to modify packets. This combination presented a reputation value to detect malicious nodes and isolate them from network participation till revocation. The approach checked nodes, including those isolated at time period l. A node that reverted from its misbehaviour was revoked to normalcy after time period l. Simulation revealed that this combination provided more security through increased packet delivery ratio and lower packet drops. Also the approach has less overhead when compared to present techniques.

A risk-aware response mechanism to cope with identified routing attacks was proposed by Zhao, et al., (2012) [13]. This was based on an extended Dempster-Shafer mathematical theory of evidence introducing importance factors. The experiments demonstrated the approach's effectiveness considering many performance metrics.

III. METHODOLOGY

ABR

Associativity Based Routing protocol in MANET family is an on-demand routing protocol whose features include using associativity ticks required for route formation based on node stability. This is due to the fact that route formation using a node which will move out of topology will be useless, as it will be broken. Thus, ABR emphasizes route longevity. Associativity ticks to signal mobile hosts' stability through beacons. Associativity is related to a mobile hosts' spatial, temporal and connection stability. It is also measured by node connectivity to surrounding nodes. A mobile host is in a high state of mobility in ABR when it has low associativity ticks with neighboring nodes. But, when associativity tick is high, the mobile host is stable; this being the ideal point to perform routine procedures. ABR includes 3 phases; route discovery, route reconstruction and route deletion [14].

Route discovery is accomplished through a broadcast query and wait a reply (BQ-REPLY) cycle. A node wanting a route broadcast a BQ message for mobiles with a destination route. Nodes which receive this query (and not the destination) append addresses and associativity ticks with neighbors with QoS information to query packet. A successor node deletes all upstream node neighbors associativity tick entries retaining only entries relating to itself and the upstream node. Thus, every resultant packet at destination contains nodes associativity ticks with destination route. The destination then selects the best route by examining associativity ticks on each path. Where many paths have similar overall association stability, a route with minimum hops number is selected. The destination then releases a REPLY packet to source on this path. REPLY propagating nodes mark valid routes. All routes are inactive and chances of duplicate packets reaching the destination is also avoided [15].

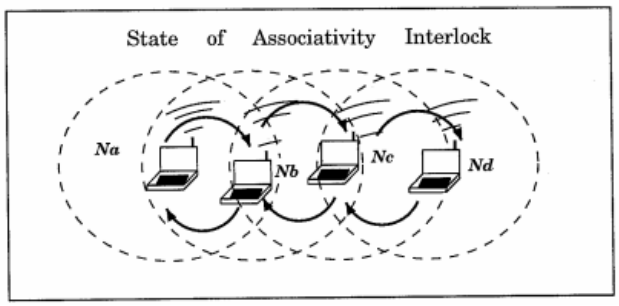

Figure 2: Interlocking phenomenon in ad-hoc mobile networks.

Denial Of Service Attacks

A Denial of Service (DoS) attack tries to prevent a victim from using all/part of his/her network connection. They can extend to all protocols stack layers. And they target service availability/authorized users' access to service providers. They have many forms and are hard to prevent. For example, an attacker may send excessive requests to a server to test legitimacy. The test needs a specific amount of CPU/memory capacity. Due to excessive requests, the server tests illegal requests and so becomes unavailable for legal users. Compared to wired networks, DoS MANET attack's damage the victim node and degrade entire network performance as nodes have limited battery power and network can be contested by limited bandwidth compared to fixed networks. [16].

Defending Against Dos Attacks

Detection and prevention are 2 schemes to handle DoS attacks. Detection is locating an attacker to initiate appropriate action. Monitoring nodes' activity or tracing an attacker helps detect a DoS attack source. Many tracing/ monitoring mechanisms including core-based/edge-based monitoring and deterministic and probabilistic packet marking were proposed in literature. Prevention mechanism thwarts DoS attacks before they take place. This is done by identifying an attack packet and initiating action before it reaches the target. Common mechanisms used on the Internet include ingress or egress filtering and route-based packet-filtering mechanisms [17]. Mobile ad hoc network systems presented dynamically and self-organized in temporary topologies are MANET networks. Internal attacks are severe as malicious insider nodes are already in the network as authorized parties and are thus protected by network security mechanisms. A modified ABR routing includes a Trap Header for malicious node identification. Experiments demonstrated that the proposed ABR performed better than ABR in the presence of DoS ATTACKS in dynamic conditions.

IV. RESULTS AND DISCUSSION

The proposed ABR is simulated to evaluate its performance and compared with traditional ABR. The simulations were conducted using 40 nodes moving in 2km X 2 km area. The experiments are conducted for varying speeds of the mobile nodes. The speed is varied from 10 Kmph to 90 Kmph and studied for the network performance. Several performance metrics compare the proposed ABR protocol with the existing ones. Metrics considered for comparison include

- Packet Delivery Ratio: the ratio of the number of packets received and number of packets sent.
- Average End to End delay: Provides mean time (in seconds) taken by packets to reach respective destinations.

Table 1 tabulates the Number of hops to destination, end to end delay and packet delivery ratio obtained for the proposed ABR. Figure 2-4 shows the same.

TABLE 1: RESULTS OF THE EXPERIMENTS

Mobility	ABR	ABR with 10% malicious nodes	ABR with 20% malicious nodes	ABR with 30% malicious nodes
	No of hops to destination			
10 Kmph	2.8	3.1	3.3	3.5
30 Kmph	3.1	3.4	3.6	3.8
50 Kmph	3.7	4.1	4.3	4.4
70 Kmph	4.1	4.4	4.7	4.7
90 Kmph	4.3	4.6	4.9	4.9
	End to End Delay			
10 Kmph	0.0514	0.0566	0.0624	0.0688
30 Kmph	0.0608	0.067	0.0738	0.0813
50 Kmph	0.0684	0.0754	0.0831	0.0916
70 Kmph	0.0726	0.08	0.0882	0.0972
90 Kmph	0.0784	0.0864	0.0952	0.1049
	Packet Delivery Ratio			
10 Kmph	0.90278	0.8279	0.7593	0.6964
30 Kmph	0.8948	0.8206	0.7526	0.6902
50 Kmph	0.8642	0.7926	0.7269	0.6666
70 Kmph	0.8321	0.7631	0.6998	0.6418
90 Kmph	0.8144	0.7469	0.685	0.6282

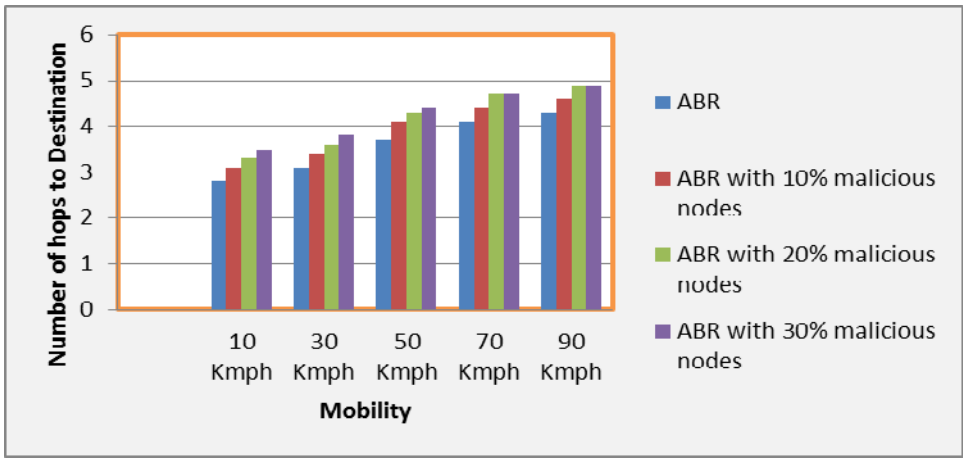

Figure 3: Number of Hops to Destination

It is observed from Table 1 and Figure 3 that Number of Hops to Destination is drastically increased by 20% between ABR and ABR with 30% malicious nodes with speed of 10 Kmph. Similarly when the speed is 90 Kmph it is increased by 12.24% between ABR and ABR with 30% malicious nodes.

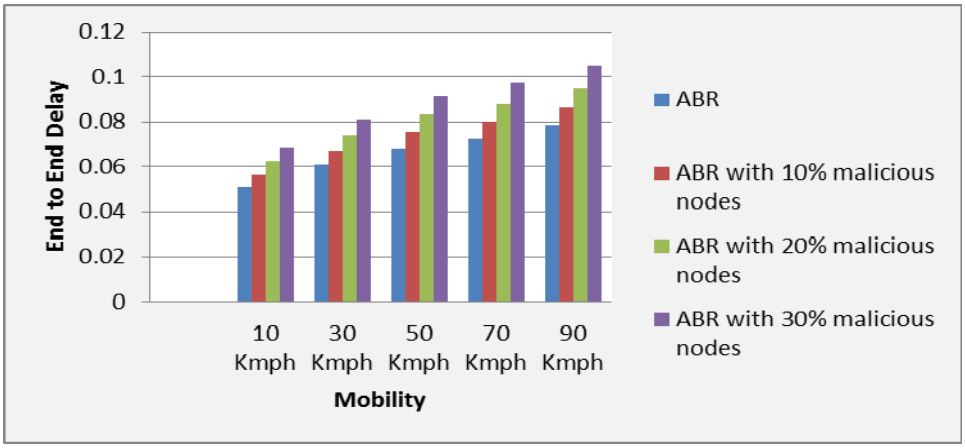

Figure 4: End to End Delay

It is observed from Table 1 and Figure 4 that End to End delay is increased by 25.29% between ABR and ABR with 30% malicious nodes with speed of 10 Kmph. Similarly when the speed is 90 Kmph, it is increased by 25.26% between ABR and ABR with 30% malicious nodes.

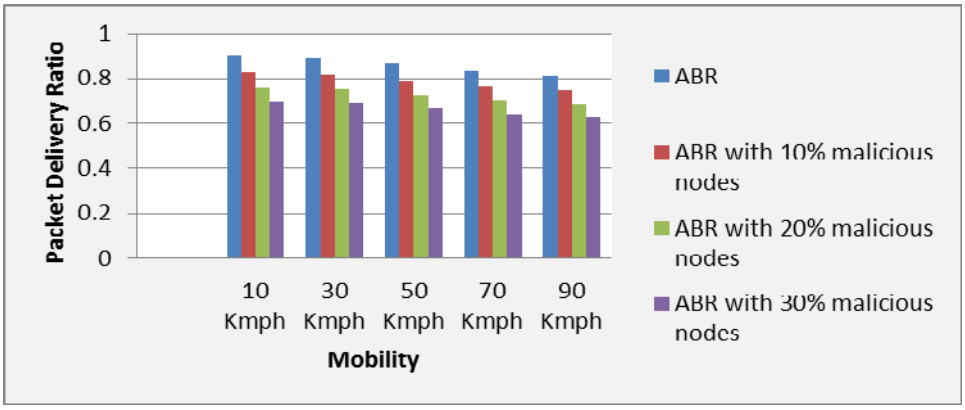

Figure 5: Packet Delivery Ratio

It is observed from Table 1 and Figure 5 that Packet Delivery Ratio is drastically decreased by 22.86% between ABR and ABR with 30% malicious nodes with speed of 10 Kmph. Similarly when the speed is 90 Kmph it is decreased by 22.86% between ABR and ABR with 30% malicious nodes.

V.CONCLUSION

MANET networks are mobile ad hoc network systems presented dynamically and self-organized in temporary topologies. Internal attacks are more severe as malicious insider nodes already belong to the network as authorized parties and so are protected by network security mechanisms. The ABR routing is modified to include a Trap Header to identify malicious nodes. Experimental results demonstrate that the proposed ABR performance better than ABR in the presence of DENIAL OF SERVICE ATTACKSunder dynamic conditions.

REFERENCE

[1] Macker, J. P., &Corson, M. S. (1999). Mobile ad hoc networking and the IETF.ACM SIGMOBILE Mobile Computing and Communications Review, 3(1), 11-13.
[2] Corson, M. S., Macker, J. P., &Cirincione, G. H. (1999). Internet-Based Mobile Ad Hoc Networking (Preprint). MARYLAND UNIV COLLEGE PARK INST FOR SYSTEMS RESEARCH.
[3] Demetrios, Z. Y. (2001). A Glance at Quality of Services in Mobile Ad-Hoc Networks. University of California, Tech. Rep.
[4] 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.
[5] Wu, B., Chen, J., Wu, J., &Cardei, M. (2007). A survey of attacks and countermeasures in mobile ad hoc networks. In Wireless Network Security (pp. 103-135). Springer US.
[6] Toh, C. K. (1997). Associativity-based routing for ad hoc mobile networks.Wireless Personal Communications, 4(2), 103-139.
[7] Kuosmanen, P. (2002). Classification of ad hoc routing protocols. Finnish Defence Forces, Naval Academy, Finland, petteri. kuosmanen@ mil. fi.
[8] Sivavakeesar, S., &Pavlou, G. (2005, January). Associativity-based stable cluster formation in mobile ad hoc networks. In Consumer Communications and Networking Conference, 2005. CCNC. 2005 Second IEEE (pp. 196-201). IEEE.
[9] Bhalaji, N., &Shanmugam, A. (2011). Defense Strategy Using Trust Based Model to Mitigate Active Attacks in DSR Based MANET. Journal of advances in information technology, 2(2), 92-98.

[10] Dadhania, P., & Patel, S. (2013). Performance Evaluation of Routing Protocol like AODV and DSR under Black Hole Attacks. Performance Evaluation, 3(1), 1487-1491.
[11] Sridhar, K. N., & Chan, M. C. (2005, October). Stability and hop-count based approach for route computation in MANET. In Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference on(pp. 25-31). IEEE.
[12] Murugan, R., &Shanmugam, A. (2010). A combined solution for routing and medium access control layer attacks in mobile ad hoc networks. Journal of Computer Science, 6(12), 1416.
[13] Zhao, Z., Hu, H., Ahn, G. J., & Wu, R. (2012). Risk-Aware Mitigation for MANET Routing Attacks. Dependable and Secure Computing, IEEE Transactions on, 9(2), 250-260.
[14] Buruhanudeen, S., Othman, M., Ali, B. M., & Othman, M. (2007). Performance Comparison of MANET Associativity Based Routing (ABR) and the Improvisation Done for a More Reliable and Efficient Routing.
[15] Donatas Sumyla "Mobile Ad-hoc Networks (manets)
[16] Soomro, S. A., Soomro, S. A., Memon, A. G., &Baqi, A. Denial of Service Attacks in Wireless Ad hoc Networks.
[17] Denko, M. K. (2005). Detection and prevention of denial of service (DoS) attacks in mobile ad hoc networks using reputation-based incentive scheme.JournalSystemics, Cybernetics and Informatics, 3(4), 1-9.