Target Detection System (TDS) for Enhancing Security in Ad hoc Network

Hoshiyar Singh Kanyal[1], Prof. (Dr.) S. Rahamatkar[2,] Dr .B.K Sharma[3,] Bhasker Sharma[4]

[1] Research Scholar, IFTM, University Moradabad, India
[2] Professor, Computer Science and Engineering (CSE), Shree Rayeshwar Institute of Engineering and Information Technology, Shiroda India
[3] Professors, Ajay Kumar Garg Engg. College (AKGEC) Ghaziabad, India,
[4]Hi-Tech Institute of Engineering & Technology, Ghaziabad, India

ABSTRACT

The idea of an ad hoc network is a new pattern that allows mobile hosts (nodes) to converse without relying on a predefined communications to keep the network connected. Most nodes are implicit to be mobile and communication is implicit to be wireless. Ad-hoc networks are collaborative in the sense that each node is assumed to relay packets for other nodes that will in return relay their packets. Thus all nodes in an ad-hoc network form part of the network's routing infrastructure. The mobility of nodes in an ad-hoc network denotes that both the public and the topology of the network are extremely active. It is very difficult to design a once-for-all target detection system. Instead, an incremental enrichment strategy may be more feasible. A safe and sound protocol should at least include mechanisms against known assault types. In addition, it should provide a system to easily add new security features in the future. Due to the significance of MANET routing protocols, we focus on the recognition of attacks targeted at MANET routing protocols.

Intrusion detection techniques for cooperation of node in MANET have been chosen as the security parameter. This includes Watchdog and Path rater approach. It also nearby Reputation Based Schemes in which Reputation concerning every node is measured and will be move to every node in network. Reputation is defined as Someone's donation to network operation. CONFIDANT [23], CORE [25], OCEAN [24] schemes are analyzed and will be here also compared based on various parameters.

KEYWORDS

MANET, CONFIDANT, CORE, OCEAN.

1. INTRODUCTION

In the recent years wireless networks [1],[18] have witnessed a tremendous increase of popularity in both research and industry. There are currently two variations of mobile networks. The first is widely known as infrastructure networks since the gateways that connect them to other networks (like the Internet) are fixed and wired.

DOI : 10.5121/ijdps.2013.4502

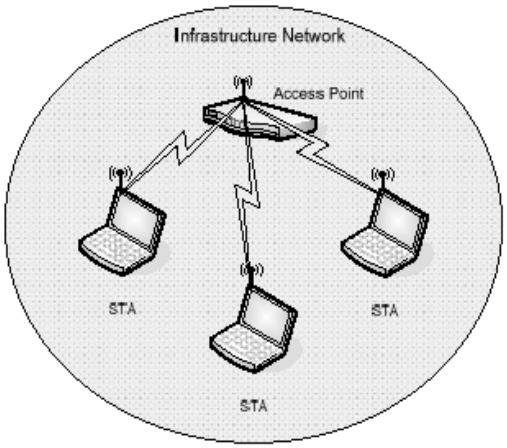

Figure 1: communications Network

In an surroundings like this, a node is able to roam freely and establish a connection link with the nearby base station that is within its communication range [2]. As the mobile node moves out of the range of the base station that it was connected with, it falls into the range of another and a handoff occurs between the old base station and the current one, enabling the mobile unit to continue communication seamlessly through the network [19] .These types of networks are most widely applied in office areas and include the wireless local area networks (WLANs)[20]. The second type of wireless networks is the infrastructureless mobile network that is also known as an ad hoc network.

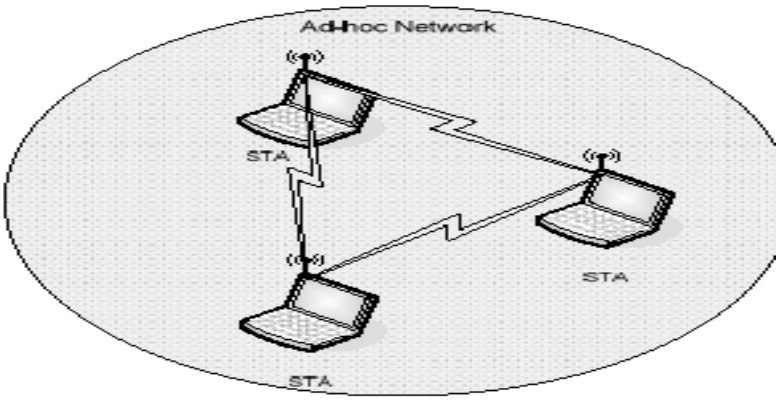

Figure 2: Adhoc Network

Infrastructureless mobile networks [18] have no fixed routers and base stations and the participating nodes are capable of movement. Due to the narrow transmission range, multiple hops may be requisite for nodes to correspond across the ad hoc network.

2. Functioning of MANET

Inside mobile ad-hoc networks where there is no communications sustain and since a target node might be out of range of a starting place node transmit packets, a routing procedure is for all time needed to find a lane so as to promote the packets appropriately between the source and the

destination. A base position can reach all mobile nodes without steering via broadcast in common wireless networks [20]. In the case of ad-hoc networks, every node must be able to sponsor data for other nodes. The following flow chart shows the working [18] of any general ad hoc network.

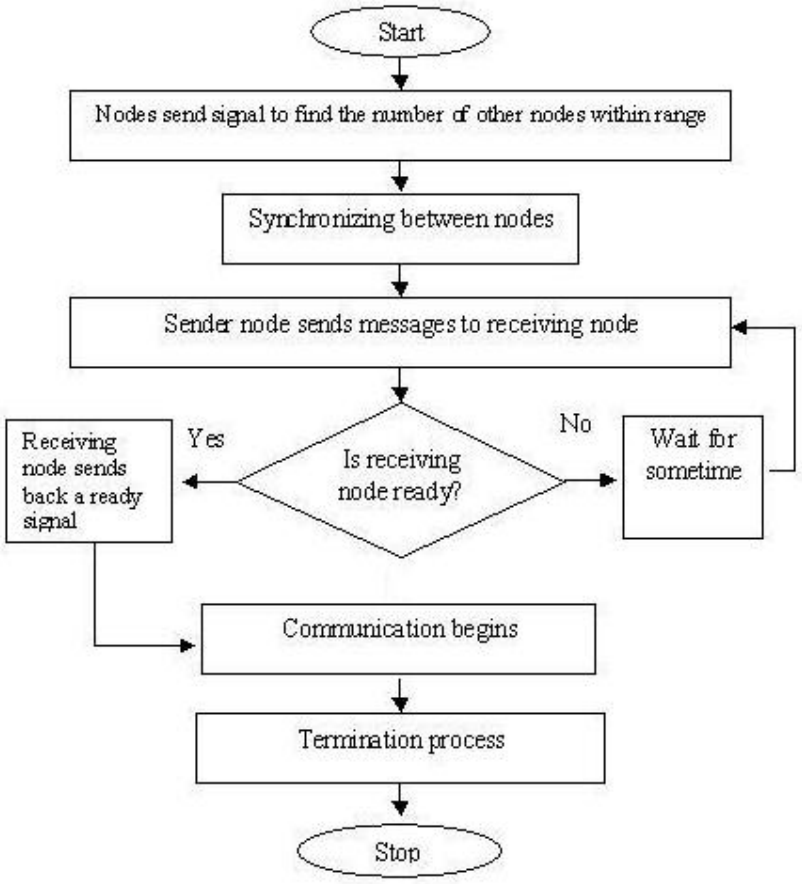

Figure 3: Functioning of MANET

2.1 Direction-Finding Protocols in Adhoc Networks

In ad hoc networking environment submission packet from a specific node may have to travel a number of hops in order to reach its destination. The major function of a routing protocol [18] is to form and preserve a routing table with in rank correlated to which the next hop for this packet should be in order to reach its critical destination. Every node has their own routing tables that they seek advice from to further the routing traffic that it is not intended for them.

Although the difficulty of routing is not a new one in computer networks, routing in ad hoc networks [22] due to its solitary necessities cannot be productively handled by exploit accessible routing schemes such as traditional link-state and distance vector routing protocols. One of the reasons that for example OSPF and RIP cannot be used in ad hoc networks [22] is that these protocols where originally designed to operate in environments with relatively static topology. However, the character of the ad hoc networks allows the participate nodes to move liberally in and out of the network.

2.2 Property of Ad hoc Routing Protocols

Since it is clear from the preceding analysis, there is a special need for routing protocols specifically intended to address the requirements of ad hoc networking. Some of the properties that ad- hoc routing protocols must posse is suggested [17] in and are analyzed given below:

- **Distributed operation**: One of the most important properties due to the decentralized nature of ad hoc networks.
- **Loop-freedom**: Even though it is not thoroughly implied that a protocol has to there loop-
- Freedom generally a desirable attribute as it usually leads to better overall performance.
- **On-demand operation**: The routing protocol as a substitute of maintain routing table entries for all the potential destinations it should rather find routes as they are required in order to conserve both energy and bandwidth.
- **Proactive operation**: It is the opposite of the "on-demand" operation. When the reactive, on-demand behavior produces unacceptable overhead in searching for routes a proactive operation is desirable.
- **Security**: It is major that the routing protocol must provide security facial appearance that prohibits the disruption or modification of network traffic.
- **Sleep**: Due to the energy constants of the participating devices of the adhoc system it is vital that the nodes have a snooze period consequential in energy conservation. The routing protocol should be able to contain such sleep periods without overly adverse consequences.
- **Unidirectional link support:** In ad hoc networks unidirectional relations can occur. The routing procedure should be able to use separate unidirectional relations in both direction to replace a bidirectional link.

3. Types of Attack in Adhoc Network

Attack is defined as **"**To begin to act upon destructively, to begin to destroy expose, alter, or disable. Attacks in adhoc network are:

3.1 Passive Eavesdrop

An attacker can listen in to any wireless network [20] to know what is disappearing on in the network. It first listen to control messages to infer the network topology to recognize how nodes are situated or are communicate with another. Therefore, it can collect smart information about the network before attacking.

3.2 Selective Existence

This malicious node which is also known as egotistic node and which is not participate in the network operation, use the network for its advantage to improve performance and save its own resources such as power. To achieve that, egotistic node puts forth its existence whenever individual cost is involved. Therefore these egotistic node behaviors are known as selective existence attacks. For example, egotistic nodes do not even send any GOODBYE messages and fall all packets even if they are sent to it, provided that it does not start the transmission. When a egotistic node wants to start a link with another node, it performs a route detection and then sends the necessary packets. While the node no longer desires to use the network, it returns to the

"noiseless mode" After a while, neighboring nodes invalidate their own route entry to this node and egotistic node becomes invisible on the network.

3.3 Gray Hole Attacks [10]

Gray hole attacks is an active attack type, which lead to falling of messages. Offensive node first agrees to promote packets and then fail to do so. Firstly the node behaves correctly and replay true RREP messages to nodes that begin RREQ message. Like this, it takes over the sending packets.
If neighboring nodes that try to drive packets over attacking nodes drop the connection to destination then they may want to discover a route again, broadcasting RREQ messages. Attacking node establish a route, sending RREP messages. This process goes on pending malicious node succeeds it's aspire (e.g. network resource consumption, battery consumption). This attack is known as routing misbehavior [10].

3.4 Black Hole Attack

The dissimilarity of Black Hole Attacks compare to Gray Hole Attacks is that malicious nodes never send true power messages initially. To bring out a black hole attack, malicious node waits for adjacent nodes to send RREQ messages. When the malicious node receives an RREQ message, without read-through its routing table, instantly sends a false RREP message giving a route to destination over itself, passing on a high sequence number to settle in the routing table of the casualty node, before other nodes send a true one. Consequently requesting nodes think that route detection process is accomplished and ignore other RREP messages and begin to send packets over malicious node.

3.5 Attacks aligned with the Routing Tables

Every node has it's possess routing table to find other nodes simply in the network. At the similar time, this routing table draws the association topology for each node for a phase (max. 3 seconds, duration of ACTIVE_ROUTE_TIMEOUT stable value of AODV protocol [6]). This attack is always performed by fabricate a new organize message. Therefore it is also named fabricating attack.

There are many attacks against routing tables. Each one is done by fabricating false control

3.6 Sleep Deprivation Torture Attack (Battery Exhaustion)

Many techniques are used to make top use of the battery life and mobile nodes similar to better to stay at the sleep mode, when they are not used. Sleep elimination Torture is one of the critical types of Denial of Service Attacks, which affects only nodes, especially handheld devices that have partial resources.

4. Target Detection System

Target or Intrusion is definite as "any set of events that effort to negotiation the integrity, confidentiality, or availability of a resource [1].Intrusion protection techniques works as the first line of defense. On the other hand, intrusion protection alone is not sufficient since there is no perfect safety in any system, particularly in the field of ad hoc networking due to its fundamental vulnerabilities. Therefore, intrusion detection [26] can work as the second line of defense to detain review data and perform traffic analysis to sense whether the network or a explicit node is under

attack. Once an intrusion has been detected in an early phase, measures can be taken to minimize the indemnity or even gather evidence to inform other genuine nodes for the intruder and maybe launch countermeasures to minimize the effect of the active attacks.

An intrusion detection system (IDS) can be confidential as network-based or host-based according to the audit data that is used. Usually, a network-based IDS runs on a entry of a network and capture and examines the network traffic that flows through it.

5. Recent work in Target or Intrusion Detection System for MANET

Mobile ad hoc network (MANET) is a self-configuring network that is produced mechanically by a collection of mobile nodes without the assist of a permanent infrastructure management. Each node is equipped with a wireless transmitter and receiver, which allow it to converse with other nodes in its radio communication assortment. In sequence for a node to forward a packet to a node that is out of its radio range, the cooperation [4] of other nodes in the network is desirable; this is called multi-hop message. Consequently, each node should act as both a host and a router at the matching time. Here are both passive and active attacks in MANETs, For passive attacks, packets containing top secret information might be eavesdrop, which violate secrecy. In Active attacks, with inject packets to ineffective destinations into the network, deleting packets; modifying the contents of packets, and impersonating other nodes violate availability, integrity, authentication, and non-repudiation. Proactive approaches such as cryptography and verification were first brought into deliberation, and many techniques have been proposed and implemented. However, these applications are not enough .Some assumptions are made in order for intrusion discovery systems to work .The first assumption are that user and program behavior are obvious. The second assumption, is that normal and intrusive activities must have discrete behaviors, as intrusion detection must confine and analyze system activity to determine if the system is under attack.

IDS can also be classified into three categories as follow.

- **Anomaly detection systems**: The normal profiles of users are kept in the system. The system compares the capture data with these profiles, and then treats any movement that deviates from the baseline as a possible intrusion by inform system administrators or initializing an appropriate response.
- **Misuse detection systems**: The system keeps pattern of known attacks and uses them to contrast with the capture data. A few matched patterns is treated as an intrusion. For example virus detection system, it cannot detect new kinds of attacks.
- **Specification-based detection**: The system defines a set of constraints that describe the exact operation of a program or protocol [26]. Then, it monitors the carrying out of the program with respect to the defined constraint.

6. Architectures of IDS in MANETs

The set of connections infrastructures that MANETs can be configured to multi-layer, depending on the applications. Therefore, the optimal IDS architecture [1] for a MANET may depend on the network infrastructure itself. In a network infrastructure, all nodes are measured equal, thus it may be appropriate for applications such as fundamental classrooms or conferences. On the contrary, some nodes are considered dissimilar in the multi-layered network infrastructure.

6.1 Stand-alone Intrusion finding Systems

In this construction, an intrusion detection [26] system is sprint on each node separately to decide intrusions. Every result made is based only on information composed at its own node, since there is no cooperation [4] between nodes in the network. Therefore, no data is exchange. In adding together, nodes in the same network do not know a little about the situation on other nodes in the network as refusal information is passed.

6.2 Distributed and supportive Intrusion Detection Systems

In view of the fact that the nature of MANETs is scattered and requires cooperation of other nodes, **Zhang and Lee [16]** have intended that the intrusion detection and reply system in MANETs should also be both circulated and cooperative as shown in Figure 4. All node participates in intrusion detection and reply by having an IDS agent successively on them. An IDS agent is responsible for detecting and collecting local trial and data to identify possible intrusions, as well as initiating a response separately. On the other hand, adjacent IDS agents willingly participate in global intrusion detection actions when the evidence is uncertain. Similarly to stand-alone IDS architecture is more appropriate for flat network infrastructure, not multi-layered one.

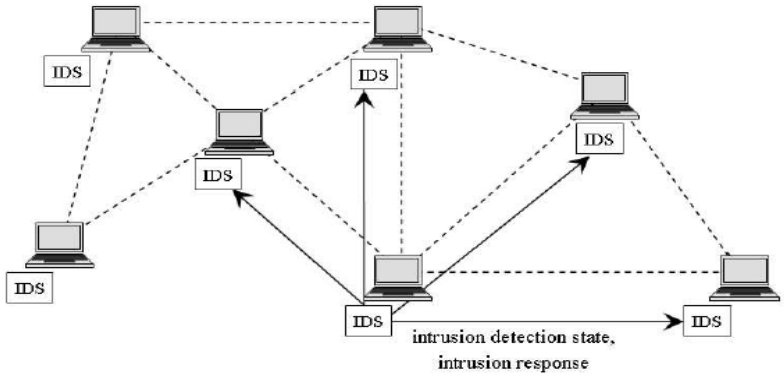

Figure:4 Distributed and Cooperative IDS in MANET proposed by Zhang and Lee**.**

6.3 Hierarchical Intrusion Detection Systems

Hierarchical IDS architectures enlarge the scattered and cooperative IDS architectures and have been planned for multifaceted network infrastructures where the network is alienated into clusters. Cluster heads of each cluster regularly have more functionality than other members in the clusters.

7. Proposed Local Reputation Based Target Detection System

Local Reputation System addresses the problem of node cooperation [4] in self organized adhoc networks. In these networks, nodes may not belong to single authority and don't have common goals. By Self Organizing mean that regular function of network depends on End Users operation.

In this Trust is associated with its reputation [21] value. There are three trust type and we use a trust worth, T_X, to represent the trustworthiness of a node. A node A considers another node B either

- trustworthy, with $T_X = 1$,
- untrustworthy, with $T_X = -1$, or
- trustworthy undecided, with $T_X = 0$

A trustworthy node [23] is a regular node that can be trusted. An untrustworthy node is a behave badly node and should be avoid. A node with undecided trustworthiness is usually a new node in the neighborhood. It may be a regular or a misbehaved node, depending on its future presentation. Every node keeps a status table, which associates a status value with each of its neighbors. It updates the reputation table based on direct surveillance only.

- $T_X = 1$,if $Rt < R < Rmax$,
- $T_X = -1$,if $Rmin < R < Ru$,
- $T_X = 0$,if $Ru < R < Rt$.

8. System Overview

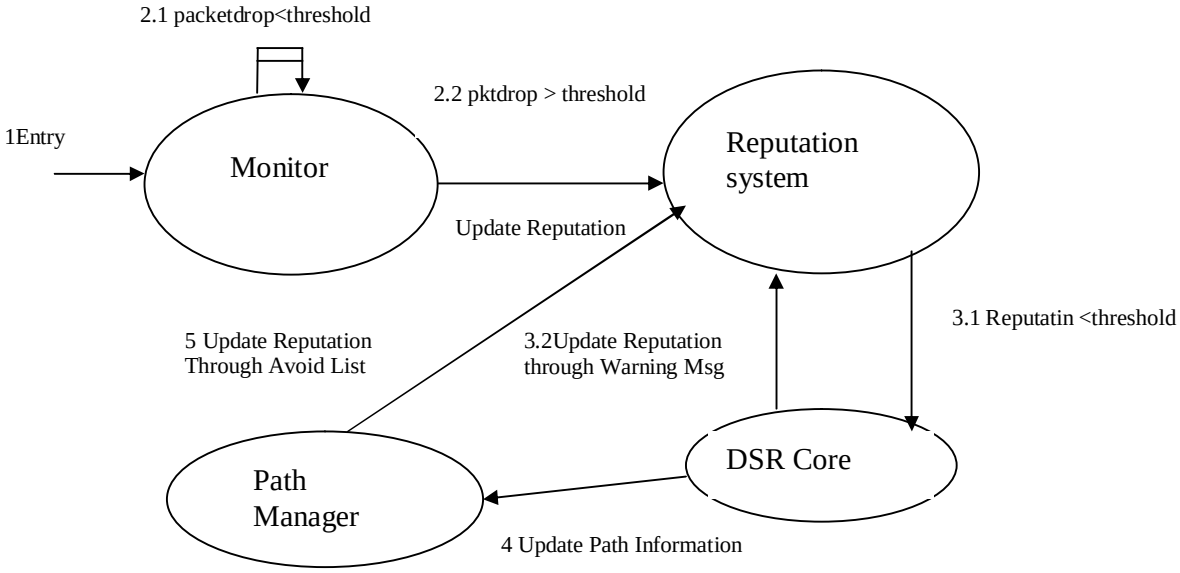

Figure 5: Target Detection System Based on Reputation

8.1 Monitor

The Monitor hold the task of monitoring behavior in the Neighborhood using Passive Acknowledgements which have been provided as a feature in the DSR[17] protocol ,provision as Promiscuous Mode. All node register all the data packets sent by it to next node and when it

receives packets in immoral mode, it matches those to the line of register packets present in its buffer.

8.2 Reputation Manager

Reputation System assigns and maintains reputation of different nodes. Each node maintains only reputation value of its one hop neighbor. With reputation of any node can alter by three means:

- By Self inspection
- Caution Message, issued by neighboring nodes.
- Avoid List, appended to the RREQ/RREP header.

8.3 Calculation and Updating of Reputation Value:

Local Reputation System [3] uses local reputation value, where each node preserves only reputation values of its one hop neighbors. The reputation value is simplified based only on its direct inspection of the neighbors; no second hand reputation information exchanged and integrated .Suppose a Node A behaves frequently. Every time it forward a message ,its one hop neighbor watch its Normal behavior and add to its reputation value by say w. Rx(A) mean Reputation Value of node A in node x reputation table.

$$Rx(A) = Rx(A) + w$$

Presume M is a malicious node and drops the communication from its previous node, N. Then there are several different cases.

Case 1: N sent a message to M but M failed to forward it.

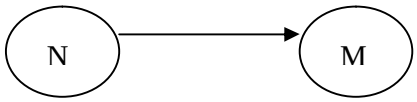

Figure 6: N Sent a message to M but M failed to forward it .

For every node X in, which is a one-hop neighbor of both N and M, X detects the misbehavior [10] and reduces the reputation value of M by y, where $y > z$. That is,

$$Rx(M) = Rx(M) - y$$

Case 2 M has forwarded the message but not forwarded trace.

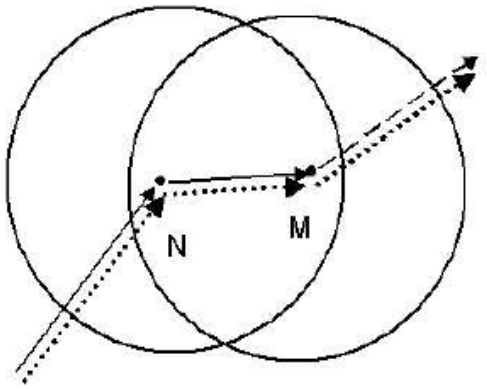

Figure7: M has forwarded the message but not forwarded trace.

Every node X, which is a one-hop neighbor of M, but not a one-hop neighbor of N, X realizes that M has not forwarded the message when it gets the outline, then X will decrease M's reputation value by y. Therefore, all one-hop neighbors of M decrease its reputation by y. i.e.

$Rx(M) = Rx(M) – y, X=Rx(M)- N(M)$

Case 3: M have not forwarded the message, and has also dropped the outline.

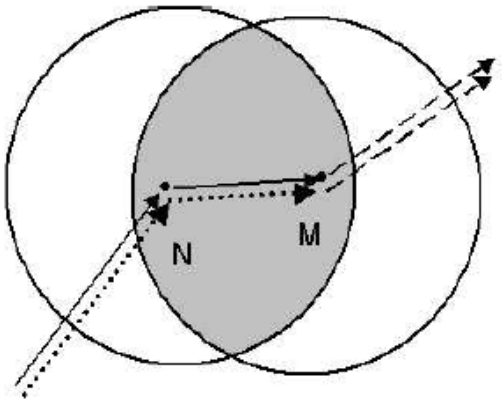

Figure 8: M has not forwarded the communication, and has also dropped the outline.

$Rx(M) = Rx(M) – t$

8.4 Path Manager

The path manager perform minor path management functions in association with DSR [17] core. Path ranking is done according to path priority formula.

8.5 Recovery and Fading

Recovery and Fading are introduced in our plan to allow nodes previously calculated malicious to become apart of the network yet again.

9. Algorithms

Subsequent algorithms give a brief idea of the Route Discovery phase, Monitoring mode and Trace test aspect of our system as discussed in earlier sections.

SENDER

1 Generate RREQ Packet
2 Packs Malicious List in RREQ Header as Avoid List
3 Propagate Request

OTHER NODES

4 if (Own name present in Avoid List) then
5 Drop Request
6 else
7 Scan Avoid List
8 Update Node's Reputation
9 Append its own malicious list to RREQ header avoiding repetition
10 if (Node is same as Destination in RREQ) then
11 Prepare Reply
12 else
13 Add itself in route and propagate
14 end if
15 end if

Algorithm for Route Discovery Phase

MONITOR MODE

Self Observation-
1 if (Performance is below normal Threshold) then
2 Negative reputation update
3 else
4 Positive reputation update
5 if (reputation is above 0) then
6 SET reputation = 0
7 end if
8 end if

WARNING MESSAGE PROPAGATION

9 if (WARNING MSG && NEIGHBOR) then
10 if (Reputation below Suspicious Threshold) then
11 Perform Trace Test

```
12 if (Trace Test is Passed) then
13 Assign normal reputation
14 else
15 declare as Malicious
16 spread Warning Message
17 end if
18 end if
19 else
20 decrease reputation
21: end if
```

Algorithm for Monitor Mode Phase**.**

Trace Test

```
1 Identify target Node
2 Generate fake data packet with route via target node
3 Send packets to target node and wait for its Passive Acknowledge (PACK).
4 if (PACK is found) then
5 tests accepted
6 Set reputations to default
7 else
8 tests unsuccessful
9 Declare node as malicious and broadcast Warning message
10 end if
```

Algorithm for Trace Test

The trace test is designed particularly for instant neighbors to test whether a exacting node is malicious or nodes in suspicious state.

10. Implementation Issues

The network simulator *ns-2* [NS03] is an object–oriented, discrete event-driven network simulator developed at the Berkley and ISC ISI as part of the VINT project [VIN03]. It is a very helpful tool for conducting network simulations concerning local and wide area networks.

The ns-2 network simulator has gained a huge status between participant of the investigate community, mainly because of its simplicity and modularity. The connection simulation allows simulation scripts, also called simulation scenarios, to be easy written in a script-like programming language TCL. More compound functionality relies on C++ code that either comes with ns-2 or any other that is supplied by the user.

11. Conclusion

Mobile adhoc networks (MANET) have a numeral of defense issues which cannot be solved without help by simple IDS. In this, we have seriously examined the offered systems and outlined their strength and shortcomings. We have opted a loom for our system in terms of mode of information propagation amongst nodes. The plan was to design a system incorporate the best behavior of all presented systems without incur further routing overhead. Trace test and Timing

window and recovery and Fading mechanism are some new concept that has been introduced in this system.

We discuss various attacks in adhoc in adhoc network. In Future to simulate Black Hole attack in adhoc network and investigate its effects. Also detection of Black Hole node is another Future work.

References

[1] S.Madhavi "Intrusion Detection in Mobile Adhoc Networks". In Proceedings of International Conference on Information Security and Assurance, vol 8, July2008, IEEE.

[2] Y.Xiao,X Shen, A Survey on Intrusion Detection in Mobile AdHoc Networks. In Proceedings of Wireless and Network Security, pp 176-190 June 2006.

[3] Sonja Buchegger and Jean-Yves Le Boudec, "Self-Policing Mobile Ad-Hoc Networks by Reputation Systems"IEEE Communication Magazine, vol. 43, No. 7, p. 101, 2005.

[4] S. Buchegger and J. L. Boudec. Performance Analysis of the CONFIDANT protocol: Cooperation of nodes Fairness in dynamic ad-hoc Networks. In Proceedings of IEEE/ACM Symposium on Mobile AdHoc Networking and Computing (MobiHoc), Lausanne, CH, June 2005.

[5] Anand Patwardhan, Anupam Joshi, Jim Parker, Michaela lorga; Secure Routing and Intrusion Detection in Adhoc Networks. In the Proceedings of the 3rd International Conference on Pervasive Computing and Communications (PerCom 2005), Kauai Island, Hawaii, July 2005.

[6] G. Vigna, S. Gwalani and K. Srinivasan, An Intrusion Detection Tool for AODV-Based Ad hoc Wireless Networks, Proc. of 20th Annual Computer Security Applications Conference (ACSAC'04).

[7] P. Michiardi, R. Molva, Core: A Collaborative REputation mechanism to enforce node cooperation in Mobile Ad hoc Networks, Institute EurecomResearch Report RR-02-062 – December, 2004.

[8] S. Buchegger and J.-Y. Le Boudec: The effect of Rumor Spreading in Reputation Systems for Mobile ad-hoc Networks" Proc. WiOpt'03(Modeling and Optimization in Mobile Ad Hoc and Wireless Networks), (2004).

[9] Sorav Bansal and Mary Baker, "Observation based cooperation enforcement in ad hoc networks" Technical Report, Stanford University, arXiv: cs.NI/0307012 v2 6 Jul (2003).

[10] Sonja Buchegger, Cedric Tissieres, Jean-Yves Le Boudec, "A Test-Bed for Misbehavior Detection in Mobile Ad-hoc Networks How Much Can Watchdogs Really Do?," Sixth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'04), pp. 102-111, (2003).

[11] S. Buchegger and J.-Y. Le Boudec, "The effect of rumor spreading in reputation systems for mobile ad-hoc Networks" Proc. WiOpt'03(Modeling and Optimization in Mobile Ad Hoc and Wireless Networks), (2003).

[12] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt. A specification-based Intrusion detection system for AODV. In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pages 125–134. ACMPress, 2003.

[13] Semih Dokurer, Y.M Erten.Performance Analysis of Black Hole Attack under Adhoc Network Proceedings of the 3rd ACM international Symposium on Mobile AdHoc Networking Computing Lausanne, Switzerland, June 09 – 11, 2002 MobiHoc '02

[14] Sonja Buchegger, Jochen Mundinger, Jean-Yves Le Boudec. Reputations System for Self Organized Network.IEEE Communications Magazine, pages 101–107, July 2002.

[15] Asad Amir Pirzada and Chris McDonald. Establishing trust in Adhoc Networks. In Proceedings of 27th Australasian Computer Science Conference, The University of Otago, New Zealand. In Research and Practice in Information TechnologyVol. 26, August 2001.

[16] C. E. Perkins, "Ad hoc Networking", Addison-Wesley, 2001.

[17] J. Broch, D. Johnson, and D. Maltz. The dynamic source routing protocol for mobile Adhoc networks. Internetdraft draft-ietf- manet-dsr-01.txt, December 1999.

[18] S. Corson, J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", Request for Comments (RFC) 2501, January 1999.

[19] J.Allen et al., State of Practice of Intrusion Detection Technologies, Tech Report CMU/SEI-99-TR-028, October 1998.

[20] Y. Xiao, X. Shen, and D.-Z. Du (Eds.). Wireless/Mobile Network Security pp. 170 – 196 . 2006 Springer.
[21] Animesh K. Trivedi, Rishi Kapoor, Rajan Arora Sudip Sanyal and Sugata Snayal: \RISM - Reputation Based Intrusion Detection System for Mobile Adhoc Networks", accpeted in CODEC'06, Kolkata, India in Dec. (2006).
[22] H. Deng, W. Li and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks". University of Cincinnati, IEEE Communication Magazine, October 2002.
[23] Jiangyi Hu," Cooperation in Mobile Ad Hoc Networks", Computer Science Department Florida State University January 11, 2005.
[24] S. Bansal and M. Baker, Observation-based Cooperation Enforcement in Ad Hoc Networks,http://arxiv.org/pdf/, July 2003.
[25] Pietro Michiardi, Rek Molva, Core: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad hoc Networks, IFIP-Communicatin and Multimedia Securtiy Conference 2002.
[26] Zhang Y, Lee W, Huang Y "Intrusion detection techniques for mobile wireless networks", 2003, A CM MONET Journal pages 3.