Journal of Mobile Communication 2 (4): 112-119, 2008
ISSN: 1990-794X
© Medwell Journals, 2008

Secured Packet Transmission in Adhoc Networks

[1]S. Varadhaganapathy and [2]A.M. Natarajan
[1]Department of IT, Kongu Engineering College, Perundurai, Erode-638052, India
[2]Department of ECE, Bannari Amman Institute of Technology, Sathyamangalam, Erode, India

Abstract: Adhoc network is a wireless temporary network, so there are more possibilities of attacks by multiple mobile intruders. Intruders may vary according to their way of attacking. Providing higher security for the mobile users is partially possible by different algorithms like approximation algorithms, distributed polynomial complexity selection algorithms, etc. Approximation algorithms requires recomputation every time the topology changes. Using analysis and simulation to find different failure rates, resource limitation and required detection rates with the applications of appropriate algorithms are partially possible. The important algorithm used in the existing system is MUNEN (Multiple Unsatisfied Neighbors in Extended Neighborhood). Active nodes in this algorithm always act as an intrusion detector in which the IDS (Intrusion Detection Software) is installed and executed within it. Selection of more number of active nodes is not possible by this algorithm. Failure to detect AODV protocol attacks, lower efficiency and higher cost of execution are some of the drawbacks of the existing MUNEN algorithm. The proposed solution uses an algorithm GODOM (GeOmetric DOMinated set) to find out more number of active nodes. The STATIDS will checkout every packet using some threshold values and if the packet transmission crosses the threshold values then that packet is marked as an abnormal packet. The proposed system has many advantages like finding more number of active nodes, improved STAT based IDS to detect more number of AODV attacks, higher efficiency and lower cost of execution. This study aims to propose an enhanced version of AODV based on GODOM algorithm and STAT-IDS.

Key words: Adhoc, active nodes, MUNEN, AODV, GODOM, STAT-IDS

INTRODUCTION

A Mobile Adhoc NETwork (MANET) is a kind of wireless adhoc network and is a self-configuring network of mobile routers (and associated hosts) connected by wireless links, the union of which forms an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily, thus the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger internet. MANET does not require any wired infrastructure for intercommunication. The nodes of MANET operate as end hosts as well as routers. They intercommunicate through single-hop and multi-hop paths in a peer-to-peer fashion. Mobile adhoc network became a popular subject for research as laptops and 802.11/Wi-Fi wireless networking became widespread in the mid to late 1990s. Many of the academic papers evaluate protocols and abilities assuming varying degrees of mobility within a bounded space. Different protocols are then evaluated based on the packet drop rate, the overhead introduced by the routing protocol and other measures.

Secured packet transmission: A strategy specifically suitable for adhoc networks is that of misuse detection that relies on the use of known patterns of unauthorized behavior (Subhadrabandhu *et al*., 2004). This technique detects intrusion when the transmitted traffic contains abnormal packets which serve as signatures of attacks. But a prerequisite for deploying misuse detection in adhoc networks is to determine which nodes should execute the sniffing and analysis software modules which we refer to as the Intrusion Detection System (IDS) modules (Denning, 1987).

The objective is to minimize the number of nodes selected for hosting packet monitoring agent subject to the requirement that every node in the network must be able to reach the monitoring nodes by at most the pre-specified number of hops that is the system parameter (Marti *et al*., 2000). The algorithms described are associates with different importance with the resource consumed by differentxx nodes selected as monitoring nodes based on their residual energy and computational capabilities.

Corresponding Author: S. Varadhaganapathy, Department of IT, Kongu Engineering College, Perundurai, Erode-638052, Tamilnadu, India

Security requirements in MANET: The security requirements in adhoc networks are similar to those in other networks. The goal is to protect information transmitted and resources in the network from malicious activities (Deng *et al*., 2002). These requirements include availability of network services, authentication of the users in order to ensure that a malicious user cannot masquerade as a trusted user, confidentiality of the information transmitted in the network, integrity of the information in order to ensure that the information is not modified by an unauthorized entity and non-repudiation in order to ensure that a node cannot refuse the sending of a message that it originated (Subhadrabandhu *et al*., 2004).

MATERIALS AND METHODS

Existing system: Active nodes is in the sense, a node act as intermediate node in which more number of packets are transmitted over it from source to destination. Active nodes are always act as an intrusion detector in which the IDS (Intrusion Detection Software) is installed and executed within it Subhadrabandhu *et al*. (2006a). The IDS is used to checkout every packet using some threshold values, if the packet transmission crosses the threshold values then that packet is marked as malicious or abnormal packet (Rao and Kesidis, 2003). The existing MUNEN algorithm uses different approaches to find the active nodes but there is some sort of collaboration occurs during the execution time in selecting the active nodes. Selection of more number of active nodes is not possible by this algorithm (Subhadrabandhu *et al*., 2006a). Failure to detect AODV protocol attacks, lower efficiency and higher cost of execution are some of the drawbacks in existing MUNEN algorithm.

Proposed system: The proposed solution uses an algorithm GODOM (GeOmetric DOMinated set) to find out more number of active nodes in a MANET. GODOM algorithm helps a node to find out number of neighboring nodes present over it and if it has more number of neighbor nodes then it is selected as an active node (Subhadrabandhu *et al*., 2006b). This algorithm will be installed with AODV protocol algorithm (Perkins and Royer, 1999), if the AODV protocol starts execution then the GODOM algorithm will also executes along with it. The proposed solution uses STAT (State Transition Analysis Technique) based IDS designed for detecting attacks against the AODV routing protocol (Subhadrabandhu *et al*., 2006a).

Geometric dominated set algorithm: The GODOM algorithm uses a special technique to find the active insider nodes called dominated set, meaning that giving supremacy to the particular nodes in which helps to monitor the network threats (Belding-Royer and Perkins, 2002). In computer science, in control flow graphs, a node 'd' dominates a node 'n' if every path from the start node to 'n' must go through 'd'. Notationally, this is written as'd dom n'. By definition, every node dominates itself.

The dominators of a node 'n' are given by the maximal solution to the following data-flow equations:

Where, 'n_0' is the start node

The dominator of the start node is the start node itself. The set of dominators for any other node 'n' is the intersection of the set of dominators for all predecessors 'p of n'. The node 'n' is also in the set of dominators for 'n'.

Dominated set pseudocode algorithm solution:

```
// Dominator of the start node is the start itself
        Dom (n_0) = {n_0}
// For all other nodes, set all nodes as the dominators
        for each n in N - {n_0}
        Dom (n) = N;
// Iteratively eliminate nodes that are not dominators
        while changes in any Dom (n)
        for each n in N - {n_0}:
      Dom (n) = {n}union with intersection over all p in pred (n) of Dom
    (p)
            Direct solution is quadratic in the number of nodes, or O (n2).
```

This algorithm, which is almost linear, but its implementation tends to be not much more complex and time consuming for a graph of several 100 nodes or less.

The proposed algorithm uses geometric information to select the IDS active insiders. This heuristic can be used in topologies where all insiders have equal transmission ranges denoted as 'r'. Thus, 2 insiders are neighbors if and only if the distance between them is less than or equal to 'r'. The network is covered by the minimum possible number of circles each with ranges 'r'. Each IDS capable insider knows or computes the coordinates of the centers of the circles. Each insider knows its coordinates (e.g., by using Global Positioning System (GPS) or other existing techniques) (Subhadrabandhu *et al*., 2006b).

An insider selects an IDS capable neighbor, which is the nearest to the center of a circle it currently resides in to execute the IDS (an insider may select itself as well since by definition it is its own neighbor) (Tseng *et al*., 2003). For this, each IDS capable insider broadcasts its distance from the center of each circle it resides in to its neighbors. It sends this broadcast packet when it joins the system and thereafter, each time it moves. GODOM detects many IDS active insiders so as to cover the entire network. Now GODOM is generalized so as to select fewer

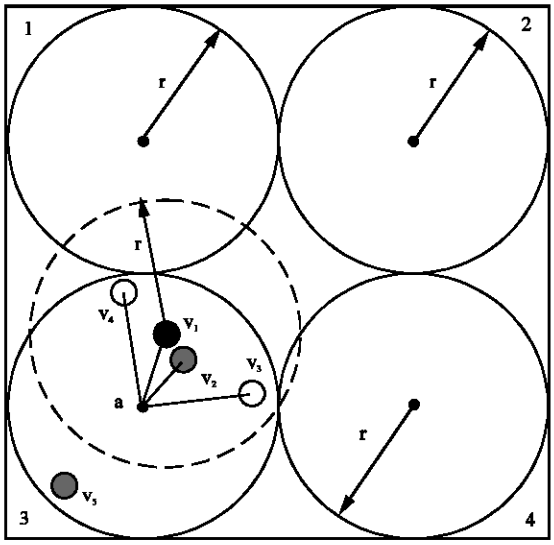

Fig. 1: Finding active nodes using GODOM algorithm

IDS active insiders at the expense of obtaining lower detection rates. Now, each insider selected by GODOM decides whether to execute the IDS with a probability which can be selected so as to regulate the resource consumed and detection rate. This version is referred as Generalized Geometric Dominating set Algorithm (GGODOM) (Subhadrabandhu *et al*., 2006b) (Fig. 1).

Existing algorithms MUNEN-IDS presents a distributed intrusion detection and response framework for mobile adhoc networks, where only few node executes the IDS and responds to intrusion (Subhadrabandhu *et al*., 2006a). The disadvantage of both these schemes is that they consume significant energy and computational resource due to involvement of every node in the detection scheme that is not efficient especially when the threat level is too high. The proposed algorithm maximizes the detection rate while minimizing the resource consumption.

The proposed system GODOM-STATIDS seeks to reduce the resource consumption by involving only a subset of nodes as monitors and provides the framework for attaining arbitrary analytical guarantee tradeoffs to the security requirements. It also proposes a fully distributed approximation algorithms to select the monitoring nodes.

GODOM-STATIDS algorithms are capable of operating in either synchronous or asynchronous fashion and also provide the guaranteeable approximation bound on the number of nodes selected as a network-monitoring sensor (Subhadrabandhu *et al*., 2006b). The algorithms also allows to associate different importance with the resource consumed by different nodes selected as monitoring nodes based on their residual energy and computational capability that have not been considered by any of the works.

Pseudocode to checkout the malicious packets

```
MYAODV1-AGENT
 void recvRequest(Packet p*)
  {
    Extract the IP_header of the packet p;
    Extract the routing information included in the packet p;
     Drop if I am the source of the packet of if I have recently heard of this
request;
      Check if I am the destination of this RREQ packet and TRESHOLD
value assigned;
 if I am the destination
      {
       send RREP;
      }
      else
      {
       drop the packet p;
      }
  }

MYAODV2-AGENT

 void recvReply(Packet p*)
  {
    Extract the IP_header of the packet p;
    Extract the routing information included in the packet p;
      Check if I am the destination of this RREP packet and TRESHOLD
value assigned;
     if I am the destination
     {
       Add the new route to the routing table;
       Further process the packet normally;
       send RREP-ACK;
     }
    else
   {
     Drop the packet;
    }
  }
```

The above specified Pseudocode is given for RREQ; RREP is given similar to the RERR and RREP-ACK messages too. The packet once checked by STATIDS and marked it as malicious then immediately dropped by it. The performance of the proposed STATIDS is higher when compared to the existing IDS's (Huang and Lee, 2004). The performance comparisons are given in graphs.

RESULTS AND DISCUSSION

GODOM-STATIDS is simulated using ns-2 to validate its efficiency and ability under volatile MANET's environments. Active node selection, Packet send, Packet Reply, Packet Drop and Packet delivery ratio were used as metrics to compare the performance of GODOM-STATIDS with MUNEN-IDS security routing algorithms (Subhadrabandhu *et al*., 2004). Each simulation result (each reported point on each curve) represents an average of 4 independent trials.

Simulation environment: In our simulation study, first 25 nodes were considered then 2 algorithms were compared by executing each. The TCL file executed first to know how many nodes were selected as active nodes from respective nodes and at the end NAM (Network AniMator) file is opened to view the network movements eventually. The nodes were increased up to 100 and the performances were calculated using 'C' file. The 'Trace.c' file is used to extract the trace file in which the packed send, received and malicious packet dropped and their delivery ratios. The nodes were divided in to static (without mobility) and dynamic (with mobility) in which their performances were calculated with the respective algorithms. The scenario files are used to make the nodes to move, send packet, pause, etc., in the MANET (Table 1).

Scenario metrics: Scenario metrics define the environment in which an adhoc network functions. These metrics do not contribute to the performance evaluation of a network, but it is critical to consider these metrics to ensure comparable results for use in any performance evaluation/comparison. We are considering the following 3 metrics:

Number of nodes, number of active nodes, node mobility and pause time.

Performance metrics: Four metrics were taken into consideration: selecting active nodes, packets send, malicious packet dropped and packet delivery ratio without malicious packet

Simulation results

Scenario for selecting active nodes: The simulation result gives number of active nodes from 25, 50, 75 and 100 set of nodes. The speed 10 m sec^{-1} and pause time 2 sec are set to constant in both algorithms. Each simulation result for GODOM-STATIDS was compared with MUNEN-IDS.

Scenario for sending malicious packet: The simulation result under attacker node sends malicious packets. The active nodes are stimulated to checkout every packet and drop it if it has the signature of attack. Different numbers of nodes from 25-100 were assigned to observe the effect of the protocol. The pause time was set to 2 sec. The speed was set to 10 min sec^{-1}. Each simulation result for GODOM-STATIDS was compared with MUNEN-IDS.

Packet send by GODOM-STATIDS and MUNEN-IDS in dynamic nodes: Packet send was same with slight variations in both the algorithms in dynamic nodes. Increasing the number of nodes by keeping all scenarios constant leads to some increases in packets sending at the stage of hundred nodes by our proposed algorithm. The Fig. 2, gives the packet send comparison ratios.

Table 1: Simulation scenario

Simulation area (grid size)	1000×1000 m
maximum number of nodes	100
Node communication range	50 m
Node initial placement	Random
Medium access mechanism	IEEE 802.11
Traffic source model	CBR
Packet size	512 Bytes
Packet rate	5 pkts sec^{-1}
Mobility model	Random waypoint
Simulation time	20 sec

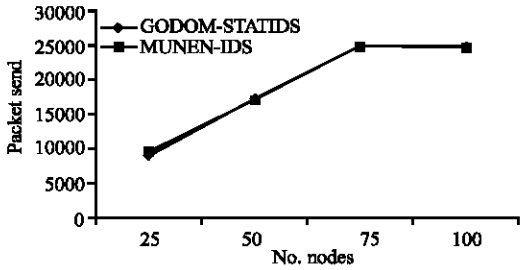

Fig. 2: GODOM vs MUNEN: Nodes vs packet send-D

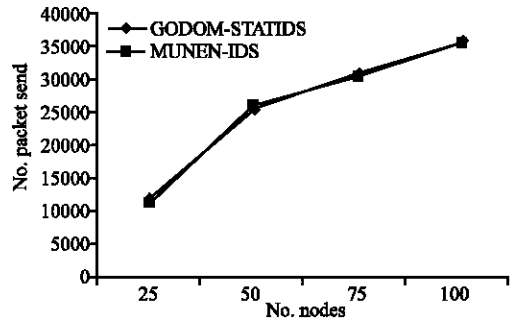

Fig. 3: GODOM vs MUNEN: Nodes vs packet send-S

Packet send by GODOM-STATIDS and MUNEN-IDS in static nodes: Packet send was same with slight variations in both the algorithms in static nodes. Increasing the number of nodes by keeping all scenarios constant leads to some increases in packets sending at the stage of hundred nodes by our proposed algorithm. The Fig. 3, gives the packet send comparison ratios.

Packet send by MUNEN-IDS (static vs dynamic nodes): Packet send was different in static and dynamic nodes (Fig. 4). Increasing the number of nodes by keeping all scenarios constant the static nodes sends more number of packets than the dynamic nodes. The node mobility

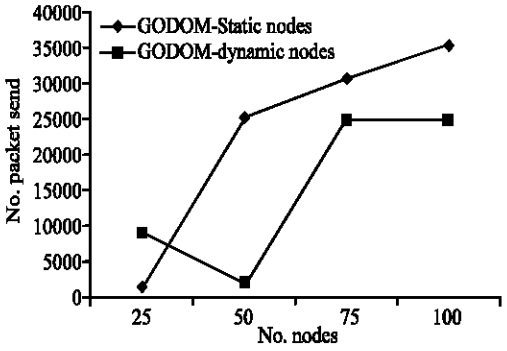

Fig. 4: GODOM: Nodes vs packet send static vs dynamic

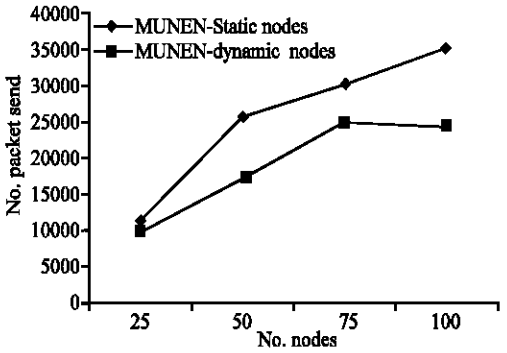

Fig. 5: MUNEN: Nodes vs packet send S vs D

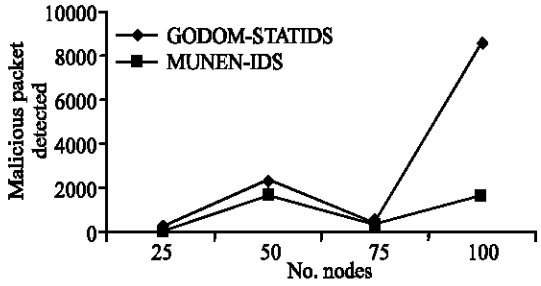

Fig. 6: GODOM vs MUNEN: Nodes vs malicious packet detected-D

was kept to zero was the main reason for more packet send. The Fig. 5 gives the packet send comparison ratios.

Malicious packet detection by GODOM- STATIDS and MUNEN-IDS in dynamic nodes: The GODOM-STATIDS algorithm detects more number of malicious packets than the MUNEN-IDS algorithm in dynamic nodes. When the number of nodes increased the detection rate was also increased in our proposed algorithm but in existing algorithm the number of nodes increased then the detection rates was decreased. The Fig. 6, gives the malicious packet detections comparison ratios.

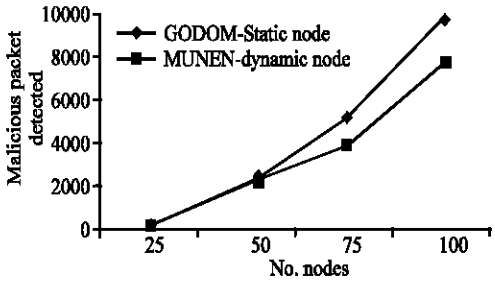

Fig. 7: GODOM vs MUNEN: Nodes vs malicious packet detected-S

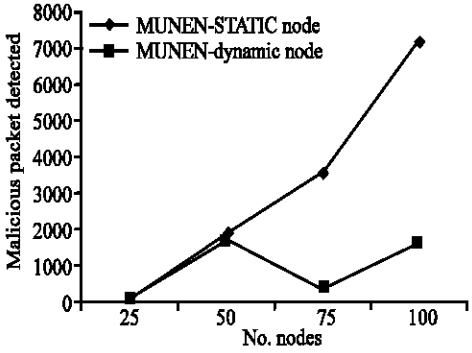

Fig. 8: GODOM: Nodes vs malicious packet detected-S vs D

Malicious packet detection by GODOM- STATIDS and MUNEN-IDS in static nodes: The GODOM-STATIDS algorithm detects more number of malicious packets than the MUNEN-IDS algorithm in static nodes. When the number of nodes increased the detection rate was also increased in our proposed algorithm but in existing algorithm the number of nodes increased then the detection rates was decreased slightly. The Fig. 7, gives the malicious packet detections comparison ratios.

Malicious packet detection by GODOM-STATIDS (static vs dynamic nodes): The GODOM-STATIDS algorithm detects more number of malicious packets in static nodes and also the detection ratio shows sequence increment when numbers of nodes have been increased but dynamic nodes shows only random detection increment ratios. The Fig. 8, gives the malicious packet detections comparison ratios.

Malicious packet detection by MUNEN-IDS (static vs dynamic nodes): The MUNEN-IDS algorithm detects more number of malicious packets in static nodes and also the detection ratio shows sequence increment when number of nodes has been increased but dynamic nodes shows only random detection increment ratios. The Fig. 9, gives the malicious packet detections comparison ratios.

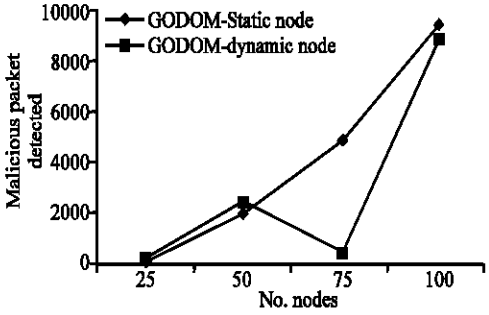

Fig. 9: MUNEN: Nodes vs malicious packet detected-S vs D

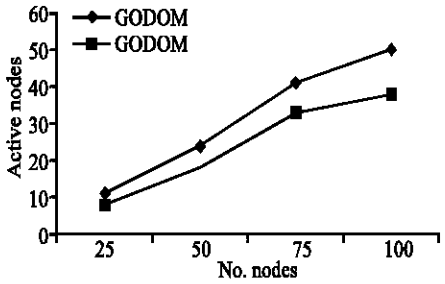

Fig. 10: GODOM vs MUNEN: Nodes vs selecting active nodes-D

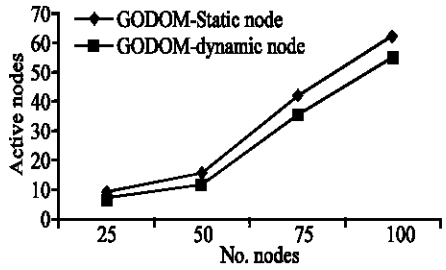

Fig. 11: GODOM vs MUNEN: Nodes vs selecting active nodes -S

Selecting active nodes by GODOM and MUNEN in dynamic nodes: The proposed GODOM algorithm selects more number of active nodes than the MUNEN algorithm in dynamic nodes. When the number of nodes increased the active node selection rate was also increased in our proposed algorithm but in existing algorithm the number of nodes increased then the active node selection rate was decreased. The Fig. 10, gives the active node selection comparison ratios.

Selecting active nodes by GODOM and MUNEN in static nodes: The proposed GODOM algorithm selects more number of active nodes than the MUNEN algorithm in static nodes. When the number of nodes increased the

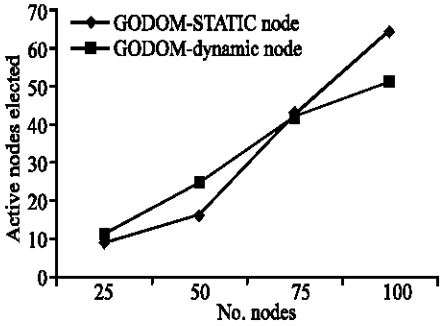

Fig. 12: GODOM: Nodes vs selecting active nodes-S vs D

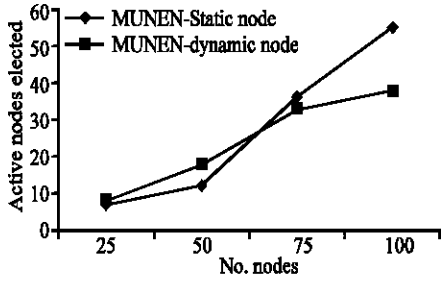

Fig. 13: MUNEN: Nodes vs selecting active nodes-S vs D

active node selection rate was also increased in our proposed algorithm but in existing algorithm the number of nodes increased then the active node selection rate was decreased. The Fig. 11, gives the active node selection comparison ratios.

Selecting active nodes by GODOM (static nodes vs dynamic nodes): The GODOM algorithm selects more number of active nodes in static nodes and also the selection ratio shows sequence increment when numbers of nodes have been increased but dynamic nodes shows only random selection increment ratios. The Fig. 12 gives the active node selections comparison ratios.

Selecting active nodes by MUNEN (static nodes vs dynamic nodes): The MUNEN algorithm selects more number of active nodes in static nodes and also the selection ratio shows sequence increment when numbers of nodes have been increased but dynamic nodes shows only random selection increment ratios. The Fig. 13 gives the active node selections comparison ratios.

Packet delivery ratio by GODOM-STATIDS and MUNEN-IDS in dynamic nodes: The GODOM-STATIDS algorithm gives more number of packet delivery ratios without malicious packets than the MUNEN-IDS algorithm in dynamic nodes. When the number of nodes increased the delivery ratio was also increased in our proposed

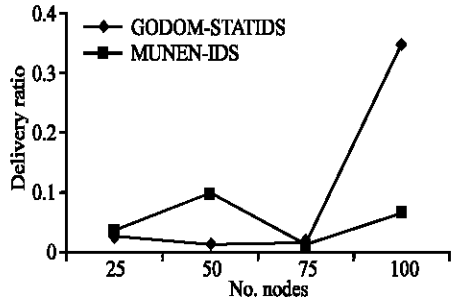

Fig. 14: GODOM vs MUNEN: Nodes vs delivery ratio-D

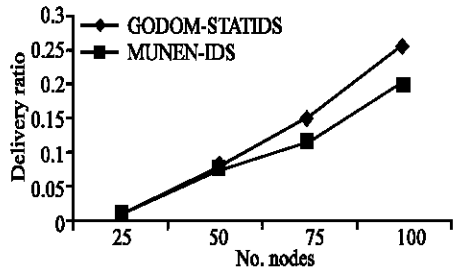

Fig. 15: GODOM vs MUNEN: Nodes vs delivery ratio- S

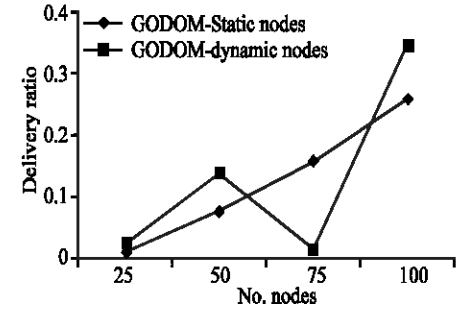

Fig. 16: GODOM-STATIDS: Nodes vs delivery ratios-S vs D

algorithm but in existing algorithm the number of nodes increased then the delivery ratio was decreased. The Fig. 14 gives the delivery ratios comparisons.

Packet delivery ratio by GODOM-STATIDS and MUNEN-IDS in static nodes: The GODOM-STATIDS algorithm gives more number of packet delivery ratios without malicious packets than the MUNEN-IDS algorithm in static nodes. When the number of nodes increased the delivery ratio was also increased in our proposed algorithm but in existing algorithm the number of nodes increased then the delivery ratio was decreased. The Fig. 15 gives the delivery ratios comparisons.

Packet delivery ratio by GODOM-STATIDS (static vs dynamic nodes): The GODOM-STATIDS algorithm gives more number of packet delivery ratios in static nodes and also the delivery ratio shows sequence increment when numbers of nodes have been increased but dynamic nodes shows only random delivery increment ratios. The Fig. 16 gives the delivery ratios comparisons.

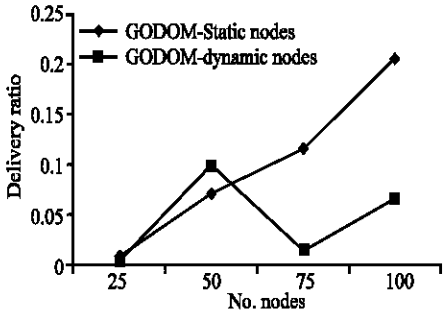

Fig. 17: MUNEN-IDS: Nodes vs delivery ratios-S vs D

Packet delivery ratio by MUNEN-IDS (static vs dynamic nodes): The MUNEN-IDS algorithm gives more number of packet delivery ratios in static nodes and also the delivery ratio shows sequence increment when numbers of nodes have been increased but dynamic nodes shows only random delivery increment ratios. The Fig. 17 gives the delivery ratios comparisons.

CONCLUSION

MANET security is the challenging task in which some research has been carried out to address this critical issue, research in this area is far from exhaustive. This project uses an algorithm GODOM (GeOmetric DOMinated set) to find out more number of active nodes in a MANET. GODOM algorithm helps a node to find out number of neighboring nodes present over it and if it has more number of neighbor nodes then it is selected as an active node. This algorithm will be installed with AODV protocol algorithm. The proposed solution uses STAT (State Transition Analysis Technique) based IDS designed for detecting attacks against the AODV routing protocol. The active nodes are only being capable in order to execute the STATIDS (Subhadrabandhu *et al*., 2004). The proposed solution maximizes performance about 40% in both static and dynamic nodes by selecting active nodes, malicious packet detections, reliable packet send and efficient packet delivery without malicious packets. Improved STATIDS detects more number of AODV attacks, higher efficiency and lower cost of execution are some of the other advantages of this project.

The GODOM-STATIDS algorithm can be implemented on the other reactive protocols like DSR and TORA. In future, more number of intruders will participate

in the network and collaborate it by attacking packets. The necessary task should be taken by improving the performances of algorithms and intrusion detection systems to prevent them by spoiling the network.

ACKNOWLEDGEMENT

I am very grateful to my supervisor who has helped me in bringing this paper to a shape for publishing. I am very thankful to my friends and students who have helped me in publishing this study.

REFERENCES

Belding-Royer, E.M. and C.E. Perkins, 2002. Transmission range effects on aodv multicast communication. ACM/Kluwer MONET, 7 (6): 455-470. http://alpha.ece.ucsb.edu/~eroyer/txt/monet.ps. DOI: 10. 1023 /A: 1020708701096.

Denning, D., 1987. An intrusion detection model. IEEE Trans. Soft. Eng., IEEE Press Piscataway, NJ, USA, 13 (2): 222-223. DOI: 10.1109/TSE.1987.232894.

Deng, H.D.P. Agrawal and W.L. Routing, 2002. Security in wireless adhoc networks. IEEE Commun. Mag., 40 (10): 70-75. DOI: 10.1109/MCOM.2002. 1039859. INSPEC: 7422917.

Huang, Y. and W. Lee, 2004. Attack analysis and detection for adhoc routing protocols. In: Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID), September, French Riviera, France.

Marti, S., T Giuli, K. Lai and M. Baker, 2000. Mitigating Routing misbehavior in mobile adhoc networks. Proc. MobiCom, pp: 255-265. ISBN: 1-58113-197-6. ACM New York, USA. DOI: http://doi.acm.org/10.1145/345910.345955.

Perkins, C.E. and E.M. Royer, 1999. AODV: Adhoc on-demand distance vector routing. In: Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp: 90-100. http://www.cs.cmu.edu/People/bumba/filing_cabinet/./papers/perkins-aodv.ps.gz.

Rao, R. and G. Kesidis, 2003. Detecting of malicious packet dropping using statistically regular traffic pattern in multihop wireless networks that are not bandwidth limited. In: Proc. IEEE GLOBECOM, 5: 2957-2961. ISBN: 0-7803-7974-8. DOI: 10.1109/GLOCOM.2003.1258776. INSPEC: 8330047.

Subhadrabandhu, D., S. Sarkar and F. Anjum, 2006a. A framework for misuse detection in adhoc networks part I. IEEE J. Sselected Areas on Communications (Special Issues on Security in Wireless Adhoc Networks), 24 (2): 274-289. DOI: 10.1109/JSAC.2005.861387. INSPEC: 8765864.

Subhadrabandhu, D., S. Sarkar and F. Anjum, 2006b. A framework for misuse detection in adhoc networks part II. IEEE J. Selected Areas on Communications (Special issues on security in wireless adhoc networks), 24 (2): 290-304. DOI: 10.1109/JSAC.2005.861388. INSPEC: 8765865.

Subhadrabandhu, D., S. Sarkar and F. Anjum, 2004. Efficacy of misuse detection in adhoc networks. In: Proceedings of IEEE SECON, 4-7: 97-107. DOI:10.1109/SAHCN.2004.1381907.INSPEC:8371304. ISBN: 0-7803-8796-1.

Tseng, C.Y. *et al*., 2003. A specification-based intrusion detection system for AODV. In: Proc. 1st ACM Workshop on Security of Adhoc and Sensor Networks (SASN), Fairfax, VA, pp: 125-134. ACM New York, USA. ISBN: 1-58113-783-4. DOI: http://doi.acm.org/10.1145/986858.986876.