International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 13, Issue 8 (August 2017), PP.46-51

A Novel Approach To Detect Trustworthy Nodes Using Audit Based Scheme For WSN

[*1]Dayanand Jamkhandikar, [2] Nagalambika S P, [3]Manikrao Mulge
[1] *Professor, CSE Department GND Engineering College Bidar, Karnataka*
[2] *M.Tech Student, CSE Department GND Engineering College Bidar, Karnataka*
[3] *Asst. Professor, CSE Department GND Engineering College Bidar, Karnataka*

Corresponding author: Dayanand Jamkhandikar

ABSTRACT: In multi-hop ad hoc networks there exists a problem of identifying and isolating misbehaving nodes which refuses to forward packets. Audit-based Misbehavior Detection (AMD) is a comprehensive system that effectively and efficiently isolates both continuous and selective packet droppers. The AMD system integrates reputation management, trustworthy route discovery, and identification of misbehaving nodes based on behavioral audits. Compared to previous methods, AMD evaluates node behavior on a per-packet basis, without employing energy-expensive overhearing techniques or intensive acknowledgment schemes. Moreover, AMD can detect selective dropping attacks even if end-to-end traffic is encrypted and can be applied to multi-channel networks or networks consisting of nodes with directional antennas. This work implements the AMD approach by considering the rushing attack. The analysis of the results confirms that AMD based method with rushing attack performs better as compared to the non rushing attack.

Keywords: Attack detection, AMD, Rushing attack, Misbehaving nodes.

I. INTRODUCTION

In the absence of a supporting infrastructure, wireless ad hoc networks realize end-to-end communications in a cooperative manner. Nodes rely on the establishment of multi-hop routes to overcome the limitations of their finite communication range. In this paradigm, intermediate nodes are responsible for relaying packets from the source to the destination; network model presupposes that intermediate nodes are willing to carry traffic other than their own. When ad hoc networks are deployed in hostile environments (tactical networks) [1], or consist of nodes that belong to multiple independent entities, a protocol-compliant behavior cannot be assumed. Unattended devices can become compromised and drop transit traffic in order to degrade the network performance. Moreover, selfish users may misconfigure their devices to refuse forwarding traffic in order to conserve energy. This type of behavior is typically termed as node misbehavior

II. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before improving the tools it is compulsory to decide the economy strength, time factor. Once the programmer‘s create the structure tools as programmer require a lot of external support, this type of support can be done by senior programmers, from websites or from books. In this paper, [2] author discussed about in mobile ad hoc networks (MANETs), an essential requirement for the foundation of communication among nodes is that nodes should coordinate with one another. In the presence of malicious nodes, this requirement may lead serious security concerns; for instance, such node may disturb the routing process. In this context, preventing or detecting malicious nodes launching rushing attack gray hole or collaborative black hole in challenge. This project attempts to determine this issue by designing a dynamic source routing (DSR)- based routing mechanism, which is referred to as the cooperative bait detection scheme(CBDS), that coordinates the advantages of both proactive and reactive defense Architectures. Our CBDS system implements a reverse tracing technique to help in achieving the stated goal. Simulation results are provided, showing that in the presence of malicious-node attacks, the CBDS outperforms the DSR, 2ACK, and best-effort fault-tolerant routing (BFTR) protocols (chosen as benchmarks) in terms of packet delivery ratio and routing overhead (chosen as performance metrics).

In mobile ad hoc networks (MANETs), a primary requirement for the establishment of communication among nodes is that nodes should cooperate with each other [3]. In the presence of malicious nodes, this necessity may lead to serious security concerns; for example, such nodes may disturb the routing process. In these contexts, preventing or detecting malicious nodes launching gray hole or collaborative black hole attacks is a challenge in mobile adhoc network. In this paper attempts to resolve this issue by designing a routing mechanism in which MD5 (Message Digest 5) technique is used. This method will help in achieving the stated

goal. In proposed work we will try to achieve packet delivery ratio and routing overhead will be considered and choosen as performance metrics.

In Mobile Ad-hoc Networks (MANETs), the main problem is the security as well as formation of communication amongst nodes is that nodes must work together with each other. Avoiding or sensing malicious nodes initiation through rushing attack gray hole or collaborative black hole attacks is the main challenge [4]. Cooperative bait detection approach mixes the advantages of both proactive and reactive defense architectures. Here it uses the technique of transposition for implementing security and the CBDA technique outfits a reverse tracing method to help in attaining the specified aim. The demonstration in the occurrence of malicious-node attacks, the CBDA outperforms the DSR, and Best-Effort Fault-Tolerant Routing (BFTR) protocols in relations to packet delivery ratio and routing overhead. In the transposition method we use the key which is the as key value of the character which is encrypted at sender side and decrypted at receiver. In paper [5] the authors proposed a system in which nodes accumulate credit to transmit their own packets. To ensure correctness, the credit reward to traffic and congestion condition, while credit-based systems motivate selfish nodes to corporate, they provide no incentive to malicious nodes .such nodes have to intend to collect for forwarding their own traffic moreover ,credit based systems do not identify misbehaving nodes, thus allowing them to remain within network indefinitely.

Routing attack to monitor and identify misbehaving nodes is considered in [6]. A node with a high packet dropping rate is given by bad reputation by its neighbors. This reputation information is propagated periodically throughout the network and is used as an important metric in selecting routes. This method can identify suspicious hops that exhibit high packet loss. Dynamic source routing (DSR) protocol for multi-hop wireless and adhoc networks is considered in [7]. Acknowledgement and cryptographic methods are used for identifying malicious nodes use of any routing protocols for detecting selective packet-dropping attacks in highly dynamic environment. The authors in [8] introduced an approach which is uses two algorithms which will be used in parallel in such a way that the results generated by one of them are further processed by other to finally generate the list of misbehaving nodes. This part detects the misbehaving links using the 2ACK.

III. SYSTEM ARCHITECTURE

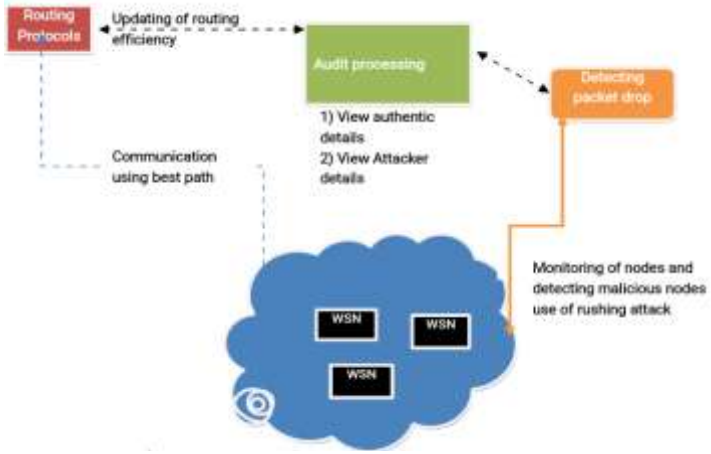

Figure 1: System Architecture

The above figure1 shows the proposed system architecture. This deals with audit processing in which it gives authentic details for detecting malicious nodes, the detection of malicious nodes done by use of rushing attack, is considered as enhancement. Initially the source node broadcasts its RREQ messages to all neighbor, source select route with highest reputation path value, mainly shorter routes are preferred [9]. The source node estimates the average of all nodes acknowledgement time called threshold value, the intermediate node rejects all paths which are having minimum threshold, is said to be attacked, the further analysis made only if there exist a path value greater in two different routes, in that case shorter route are preferred. Use of routing protocols such as AODV, DSR etc. communication done through WSN.

IV. METHODOLOGY

In multi-hop ad hoc networks there exists a problem of identifying and isolating misbehaving nodes which refuses to forward packets. Audit-based Misbehavior Detection (AMD) is a comprehensive system that effectively and efficiently isolates both continuous and selective packet droppers [9].The AMD system integrates reputation management, trustworthy route discovery, and identification of misbehaving nodes based

on behavioral audits. Compared to previous methods, AMD evaluates node behavior on a per-packet basis, without employing energy-expensive overhearing techniques or intensive acknowledgment schemes. Moreover, AMD can detect selective dropping attacks even if end-to-end traffic is encrypted and can be applied to multi-channel networks or networks consisting of nodes with directional antennas. The absence of a supporting infrastructure, wireless ad hoc networks realize end-to-end communications in a cooperative manner [10]. Nodes rely on the establishment of multi-hop routes to overcome the limitations of their finite communication range. In this paradigm, intermediate nodes are responsible for relaying packets from the source to the destination. This network model presupposes that intermediate nodes are willing to carry traffic other than their own. When ad hoc networks are deployed in hostile environments (tactical networks), or consist of nodes that belong to multiple independent entities, a protocol-compliant behavior cannot be assumed. Unattended devices can become compromised and drop transit traffic in order to degrade the network performance. Moreover, selfish users may misconfigure their devices to refuse forwarding traffic in order to conserve energy. This type of behavior is typically termed as node misbehavior as shown below in figure2.

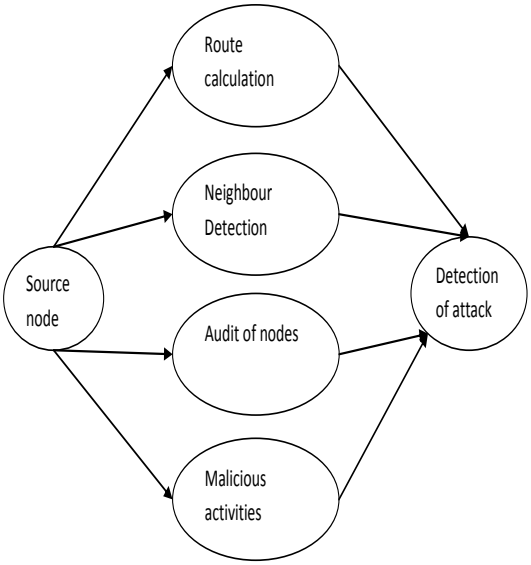

Figure 2: Use Case diagram

Implementation

Network simulator 2 is used as the simulation tool in this project. It has an open source code that can be modified and extended and is an object–oriented, discrete event simulator for networking and provides substantial support for simulation. It is written in C++, with an Otcl interpreter as a command and configuration interface. C++ is a compiled programming language needs to be compiled (i.e., translated) into the executable machine code where as Otcl is an interpreted programming language [11]. Upon execution, the interpreter translates Otcl instructions to machine code understandable to the operating system line by line.

To perform simulation and evaluate the performance following simulation parameters are used:

Simulator	NS2
Channel type	Channel/Wireless channel
Radio propagation n model	Propagation/Two ray ground
Network interface type	Phy/wireless Phy
MAC type	MAC/802_11
Interface queue type	Queue/Drop Tail/Pri Queue
Link layer type	LL
Antenna model	Antenna/Omni antenna
Max packet in ifq	300
Number of mobile nodes(nn)	50
Routing protocol	AODV
X dimension of topography	1670
Y dimension of topography	1200
Set opt initial energy	100

Table1: Parameters used

V. RESULTS AND DISCUSSION

The simulation was carried out by using the above parameters. The following evaluation metrics are considered.

- Throughput.
- Delay
- Overhead
- Packet delivery ratio(PDR)

The below table 2 show the parameters and the resulting graph by considering the X-graph tool.

Results

Parameters	Without rushing	With rushing
Throughput (kbps)	160.70	174.80
Delay(msec)	28.2001	83.20
PDR (%)	0. 9792	0. 98
Overhead(load)	2.922	3.106

Table 2: parameters graph for plotting

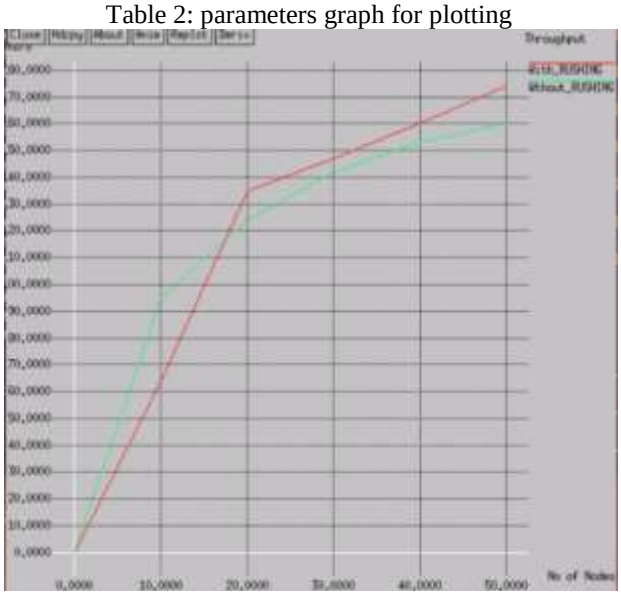

Figure 3: Throughput comparison Graph

The figure3 shows that, X-graph explains about throughput in terms of time more amount of data is transferred i.e. throughput increases, 174 bits are transmitted in. This is one of the advantages of improving network throughput.

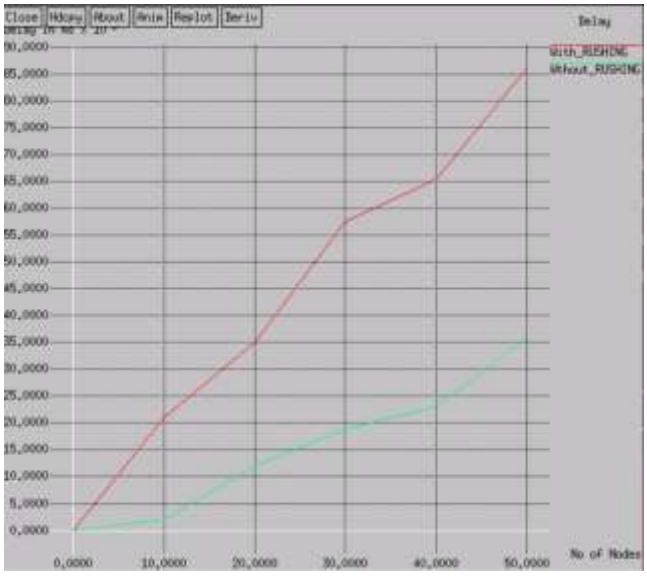

Figure 4: Average end to end delay graph

The figure4 shows that the end to end delay is calculated using difference in sent and received time, measured in mili seconds or micro seconds. Includes all possible delays caused by buffering during route discovery at queuing significant in understanding the delay introduced by path discovery.

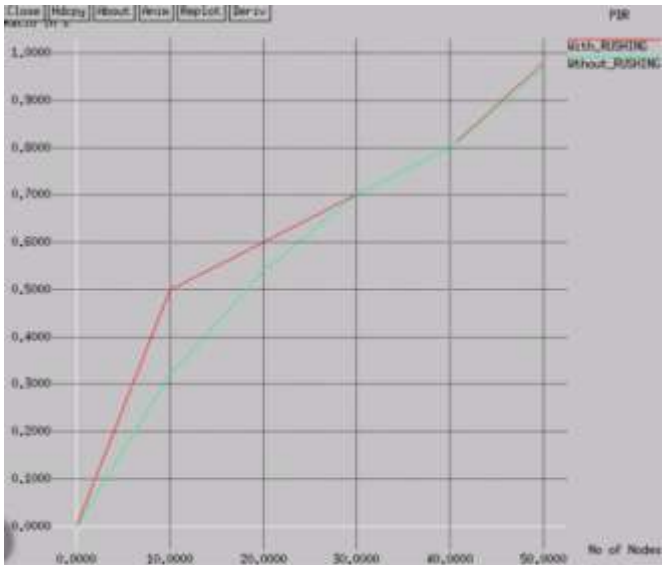

Figure 5: Packet delivery ratio (PDR) comparison graph

The figure5 shows that, PDR for total packet sent by total packet received, measured in percentage (%). Represents value for packet delivery ratio. The number of packets transmitted by source and the number of packets acknowledge by destination.

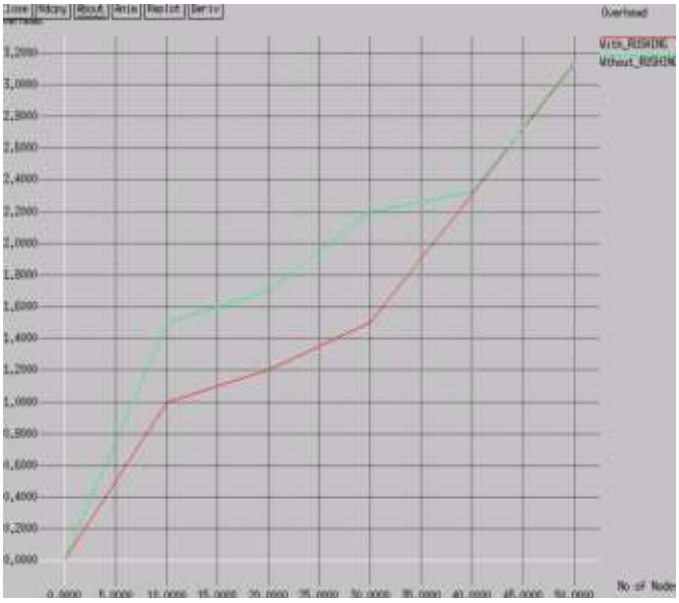

Figure 6: Overhead comparison graph

The figure 6 shows that, the number of packet processed, measured in terms of load.

VI. CONCLUSION AND FUTURE ENHANCEMENTS

This work focuses on identifying the set of nodes that misbehave in a particular path, from source to the destination. This deals with audit processing, in which it gives authentic details for detecting malicious nodes. The detection of malicious nodes is done by using rushing attack. Initially the source node broadcasts its RREQ packet to all neighbors. Source select path with highest reputation path value, mainly shorter routes are preferred. The various parameters such as throughput, delay, PDR and overhead conforms this method of AMD by using rushing attack performs better as compared to the methods without rushing attack. For better performance combine rushing attack with warm hole attack gives good results in future.

.

ACKNOWLEDGMENT

We indebted to management of GNDEC, Bidar for excellent support in completing this work at right time. A special thanks to the authors mentioned in the references.

REFERENCES

[1]. J.crowcroft, R.Gibbens, F.Kelly, and S.Ostring.modelling incentives for collaboration in mobile adhoc networks. In proceeding of WiOpt, 2010.
[2]. C. Chang, Y.Wang, and H. Chao, in mobile ad hoc networks (MANETs), an essential requirement for the foundation of communication among nodes is that nodes should coordinate with one another.IEEE explorer ,2009
[3]. A. Baadache and A. Belmehdi, in mobile ad hoc networks (MANETs), a primary requirement for the establishment of communication among nodes is that nodes should cooperate with each other.IEEE explorer 2010
[4]. K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan In Mobile Ad-hoc Networks (MANETs), the main problem is the security as well as formation of communication amongst nodes is that nodes must work together with each other.IEEE explore 2013.
[5]. L.Buttyan and J.P.Hubax.simulating cooperation in self organizing mobile adhoc networks.ACM/KLuwer mobile networks and applications, 8(5):579-592, Oct 2010.
[6]. J.Eriksson,M.Faloutsos,andS.Krishnamurthy.Routing amid colluding attackers.2010
[7]. D.B.Jhonson, D.A.Maltz, andJ.Broch.DSR: dynamic source routing protocol for multi-hop wireless and adhoc networks.2010.
[8]. Shirin Samreen, G.Narsimha (2014), an efficient approach for the Detection of Node Misbehavior in an MANET based on link Misbehavior, 2013 3rd IEEE.
[9]. Tao Shu and Marwan Krunz.Privacy- Preserving and truth full detection packet dropping attacks in wireless adhoc networks ,IEEE Transactions on mobile adhoc networks,july 2014.
[10]. Vasantha.V, Dr.Manimegalai (2010), Mitigating Routing Misbehaviors using Subjective Trust Model in Mobile Ad hoc Networks, IEEE.
[11]. C.perkins and p.bhagwat proactive protocol in MANET, M.Greis.Tutorial for the network simulator NS2, available at: http://www.isi.edu/nsnam/ns/tutorial.

*Dayanand Jamkhandikar. "A Novel Approach To Detect Trustworthy Nodes Using Audit Based Scheme For Wsn." International Journal of Engineering Research and Development, vol. 13, no. 08, 2017, pp. 46–51.