ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 2, pp: (319-327), Month: April - June 2016, Available at: www.researchpublish.com

A Secure Intrusion Detection System For Manets By Using Smart Jamming And Cryptography

Muthamil Sudar.K[1], Jaya.S.S[2], Aanandha Nachiar.K[3]

[1,3]PG Scholar, [2] Assistant Professor, [1,2,3]Department of Computer Science & Engineering, [1,2]RVS College of Engineering and Technology, Coimbatore, [3]Mahakavi Bharathiyar College of Engineering and Technology,Vasudevanallur.

Abstract: **Mobile Ad hoc Network (MANET) is one amongst the foremost necessary and distinctive applications. MANET doesn't need a set of network infrastructure; each single node acts as a transmitter and a receiver and they trust their neighbors to relay messages. Nodes can communicates directly with one another if the communication range is small otherwise make use of relay nodes. The self-configuring ability of nodes in MANET makes it more popular and used in applications like military use or emergency recovery. Unfortunately, the open medium and remote distribution of MANET leads to numerous kinds of attacks. So, it is difficult to develop successful intrusion-detection mechanisms to protect MANET from attacks. The proposed smart jamming algorithm helps to increase the system secrecy capacity. The key exchange and encryption mechanism with the help of IBS scheme provides the additional security and forward data among the nodes. RREQ and RREP process helps to detect the malicious node in the transmission and mark the detected node in the block table. The nodes are organized in spanning tree fashion in order to avoid forming cycles.**

Keywords: **transmitter, receiver, jamming, RREQ, RREP.**

I. INTRODUCTION

MANET (Mobile Ad hoc Network) is an infrastructure less wireless network where mobile nodes can move freely and can form network. These networks don’t have infrastructure and the communication occurs within the transmission range due to limited resource of energy for each node. Routing Protocols play an important role in MANET for connectivity between nodes for transfer of data packets between each node in the network and can be classified into Proactive routing protocols, Reactive routing protocols and Hybrid routing protocols. Proactive routing protocols uses routing table and exchanges link information in between nodes. Reactive protocol establishes routes only when nodes are ready to communicate means nodes does not exchange routing information. Hybrid combines the features of both proactive and reactive routing protocols. Due to the absence of centralized authority MANET is more susceptible to attacks by selfish nodes or malicious nodes. Wireless networks have gained great popularity. Providing security is a critical issue. An Adversary is empowered to launch a severe DoS attack by blocking the wireless medium- Jamming. A set of relay nodes can be exploited by multiple source-destination pairs to achieve physical layer security. Each node evaluates neighbouring nodes in order to reduce the untrusted routes and providing secure cooperative communication for MANETs via cooperative relaying and jamming. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

II. RELATED WORK

Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks: This paper describes about providing Secure data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. In this paper, they study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. They propose two secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the identity-based digital signature (IBS) scheme and the identity-based online/offline digital signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. They show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The results show that the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

Enhancing Security for Mobile Ad hoc Networks by Using Identity Based Cryptography: This paper studies key management and security issues in mobile ad hoc networks (MANETs). Lack of strong identification results in unauthorized entities access to the sensitive data, and leads to loos of confidentiality and integrity, which causes many vulnerabilities and attacks in the network .We present the key management scheme as a combination of Identity-Based (User’s Identification), Unique Transmission’s time Factor and Threshold Cryptography for ad hoc networks. It is a certificateless solution which eliminates the need for public key distribution and certificates in public key management schemes. This scheme is also efficient in computation since small unique factor enhance the authentication of entities. Generally, routing protocols are classified into three categories: Proactive, Reactive and Hybrid protocol. In proactive protocol, all the nodes maintain routing table and routing information are always available. In reactive protocol, finding a route is done by route request rather than finding route in advance.Mobility in MANET leads to lack of many security measures, which is used in conventional wireless network with the fixed infrastructure. Security attacks can be deployed in any network layers.

The Relay–Eavesdropper Channel: Cooperation for Secrecy: In facilitating secure wireless communications the four-terminal relay–eavesdropper channel is introduced and an outer-bound on the optimal rate-equivocation region is derived. Several cooperation strategies are then devised and the corresponding achievable rate equivocation region are characterized. Of particular interest is the novel noise-forwarding (NF) strategy, where the relay node sends codewords independent of the source message to confuse the eavesdropper. This strategy is used to illustrate the deaf helper phenomenon, where the relay is able to facilitate secure communications while being totally ignorant of the transmitted messages. Furthermore, NF is shown to increase the secrecy capacity in the reversely degraded scenario, where the relay node fails to offer performance gains in the classical setting. The gain offered by the proposed cooperation strategies is then proved theoretically and validated numerically in the additive white Gaussian noise (AWGN) channel**.** Our main idea is to exploit user cooperation in facilitating the transmission of confidential messages from the source to the destination. More specially, they consider a four-terminal relay–eavesdropper channel, where a source wishes to send messages to a destination while leveraging the help of a relay node to hide those messages from the eavesdropper. The eavesdropper in our model can be viewed as the wireless counterpart of Wyner’s wiretapper. This model generalizes the relay channel and the wiretap channel.

An Optimal Algorithm for Relay Node Assignment in Cooperative Ad Hoc Networks: Recently, cooperative communications, in the form of having each node equipped with a single antenna and exploit spatial diversity via some relay node’s antenna, is shown to be a promising approach to increase data rates in wireless networks. Under this communication paradigm, the choice of a relay node (among a set of available relay nodes) is critical in the overall network performance. In this paper, they study the relay node assignment problem in a cooperative ad hoc network environment, where multiple source–destination pairs compete for the same pool of relay nodes in the network. Our objective is to assign the available relay nodes to different source–destination pairs so as to maximize the minimum data rate among all pairs. The main contribution of this paper is the development of an optimal polynomial time algorithm, called ORA, that achieves this objective. A novel idea in this algorithm is a “linear marking” mechanism, which maintains linear complexity of each iteration. They give a formal proof of optimality for ORA and use numerical results to demonstrate its capability.

III. PROPOSED WORK

Our proposed system investigates the secure cooperative communication issue for wireless ad hoc networks with the presence of multiple malicious eavesdroppers. Specifically, we consider a MANET consisting of N individual nodes, with each node being a source node, a destination node, a potential relay node or an eavesdropping node. We assume that there are Ns source nodes forming the source. Each source node is required to transmit packets to its respective destination. Cooperative wireless networking with the objective to improve the system capacity has attracted extensive attentions during the past half-decade. The objective to support emergency services in MANETs, Han et al. proposed two novel networking framework for cooperative and non-cooperative MANETs. Considering physical layer security for secure cooperative communication, Dong et al. proposed effective decode and- forward (DF) and amplify-and-forward (AF) based cooperative relaying protocols for physical layer security. Recently, there have been considerable efforts devoted to generalizing physical layer security to the wireless fading channel and to various multi-user scenarios. Multiple users communicate with a common receiver in the presence of an eavesdropper, and the optimal transmission power allocation policy with cryptography is chosen to maximize the secrecy sum-rate. Used cooperative relays to improve wireless physical layer security in the presence of multiple eavesdroppers.

Advantages:

- In our proposed network, each source-destination pair can use either direct transmission or cooperative communication with the help of the best relay to achieve full diversity.

- System obtain the maximum secrecy capacity can exploit maximizing the achievable capacity of the primary channel and minimizing that of the eavesdropping channel at the same time.

IV. IMPLEMENTATION METHODOLOGY

Modules

It mainly consists of four modules. They are

- Network formation
- Key distribution
- Route selection
- Smart jamming algorithm

Module Description

In this module, investigate the secure cooperative communication issue for wireless ad hoc networks with the presence of multiple malicious eavesdroppers. Specifically, we consider a MANET consisting of N individual nodes, with each node being a source node, a destination node, a potential relay node or an eavesdropping node. Based on the antenna coverage, number of nodes will be calculated. Identify Source and destination nodes.

Key Didtribution

In this module, an optimized encryption method which may be related with the RSA key generation and Diffie Hellman key exchange mechanism, to provide more security for data exchange. In this we perform spliting both, plaintext before encryption and cipher text after encryption and also here we try to provide more security by combining both algorithms.

Route Selection

The basic idea of secure CC is that after amplifying or decoding the signals, the cooperative relay and source can beam-form towards the destination to enable a greater capacity gain in the primary channel than the eavesdropping one. According to the previous formulations, it is not easy to observe whether cooperative relay assignment can benefit the secrecy capacity. In this section, analyze the secrecy capacity gain brought by cooperative relay assignment and exploit the opportunities of secrecy capacity enhancement.

Smart Jamming Algorithm

In order to reduce the capacity of the eavesdropping channel, cooperative jamming technique which encourages one or more involved nodes to generate artificial interference towards the eavesdropping nodes is of great interests recently. It has been shown that, by carefully scheduling the interaction between relay nodes and jamming nodes, substantial secrecy improvements can be achieved. In this section, we exploit the advantages of cooperative jamming technique and propose a smart jamming algorithm to further increase the system secrecy capacity.

Ibs Scheme for Key Distribution

An IBS scheme implemented for CWSNs consists of the following operations, specifically, setup at the BS, key extraction and signature signing at the data sending nodes, and verification at the data receiving nodes:

- **Setup:** The BS (as a trust authority) generates a master key msk and public parameters param for the private key generator (PKG), and gives them to all sensor nodes.
- **Extraction:** Given an ID string, a sensor node generates a private key sekID associated with the ID using msk.
- **Signature signing:** Given a message M, time stamp t and a signing key _, the sending node generates a signature SIG.
- **Verification:** Given the ID, M, and SIG, the receiving node outputs “accept” if SIG is valid, and outputs “reject” otherwise.

Rreq and Rrep Process for Route Selection

S first checks its route table to determine whether it already has a route to D. If such a route exists, it can use that route for packet delivery, otherwise route discovery is needed. Route discovery process consists of following processes. In this section mainly discussed our two proposed algorithm, with the following set of

symbols:

i. S = Source node, D = Destination node CN= Current node, RP = Reverse Parent IP,

FP = Forward Parent IP

ii. IR =Intermediate Routers or nodes between S and D.

iii. RREQ = Route Request message, RREP = Route Reply.

iv. RREQ ID.s.id, RREQ ID.dis.id = Route Request id with corresponding extension.

(.s.id)_S broadcasts first time for 1hop destination. (.dis.id)_S broadcasts second time for multi hop destination to discover route.

RREP ID.s.id, RREP ID.dis.id = Route Reply id with corresponding extension.

(.s.id)_It is for one-hop destination node. (.dis.id)__It is for multi-hop destination node.

v. RT = Routing Table. vi. RREQ_RP = RREQ parameter: <S, D, hop count, sequence number, RP, RREQ ID>.

vii. TR = Transmission Range of a node

viii. Nack = Acknowledgment to ensure that destination has received the RREQ and to inform other non transmitted nodes not to transmit further identical RREQ and discard it.

RREQ Process:

1. S broadcasts the RREQ of (RREQ ID.s.id) first.

1a. If D is in the TR of S, then S sends the RREQ directly to the D.D returns RREP of unique ID (RREP.s.id) to the S, within (TRREQ.s+TRREP.s). Other 1hop nodes are not D and they check the extension part of the RREQ ID, if it is (.s.id) then they discard it.

1b. Else If S does not receive RREP of unique ID (RREP.s.id) from D within (TRREQ.s+TRREP.s), then it broadcasts the RREQ of unique ID (RREQ.dis.id) to find the D. IR receive this and check the extension part of the RREQ ID , if it is

(.dis.id) then they pass it until the D is found. IR and D store the RP, which is next hop to the S from CN (While forwarding RREQ, S does not need to store the RP) and also stores the RREQ ID. All nodes maintain the RREQ_RP. All nodes which have already broad-casted RREQ once, discard identical RREQ till 2TRREQ.dis after broadcasting RREQ.

2. When D receives a RREQ of unique ID (RREQ.dis.id), it discards identical RREQ till 2TRREQ.dis. After receiving first RREQ, D broadcasts Nack to stop unnecessary further broadcasting of identical RREQ. After receiving Nack other nodes, which have not broadcasted identical RREQ. All IR which have already

broadcasted RREQ once, discard Nack of same ID.

RREP Process:

3. When D receives first RREQ, it initiates RREP.

3a. If S is in the TR of D, then D sends the RREP of unique ID (RREP.s.id) directly to the S, within the time

(TRREQ.s+TRREP.s).

3b. Else D places the IP address of S, as well as its own IP address into the RREP of unique ID (RREP.dis.id) and then D sends it to its RP which is next hop to the S. The RP of D is now the CN. This CN places its own IP into the RREP of unique ID (RREP.dis.id) and then it will send the RREP to its RP. This procedure continues

until the S is reached. In RREP process, no need to maintain any parent information

Transmission Model with Jamming Algorithm

Modify the two-phase cooperative communication transmission model. Under the modified model, one or more relays that were not assigned to any s-d pairs during the assignment procedure can be selected to act as friendly jammer(s) to further increase the system secrecy capacity. During the broadcast phase, in order to protect the source's broadcast message, a relay node is selected to act as the friendly jammer, which generates intentional interference towards the eavesdropping nodes. During the cooperative phase, the assigned cooperative relay transmit the source's message towards the destination. The selected jamming relay node acts as a friendly jammer to the s-d pair it is serving, and continues to generate intentional interference towards the eavesdropping nodes. Take the network in Fig.1 as an example, relay node r_4 is not assigned to any s-d pairs after the relay assignment procedure, so it can be selected to serve as a friendly jammer for hs_1, d_1i. During the cooperative phase, the assigned cooperative relay node r_2 transmits the data from s_1 to d_1. r_4 acts as a friendly jammer to hs_1, d_1i and generates intentional interference towards eavesdropper e_2. One should also notice that the interference signal generated by the selected jamming relay node can also affect the cooperative links, for example, there is interference from r_4 to d_1 during both phases. Following our system model, orthogonal channels are applied to all s-d pairs, the selected friendly jammer can use the same channel as the s-d pair it is serving but just generating artificial interference. Thus, the interference signal generated by the friendly jammer will not affect the transmission of other s-d pairs.

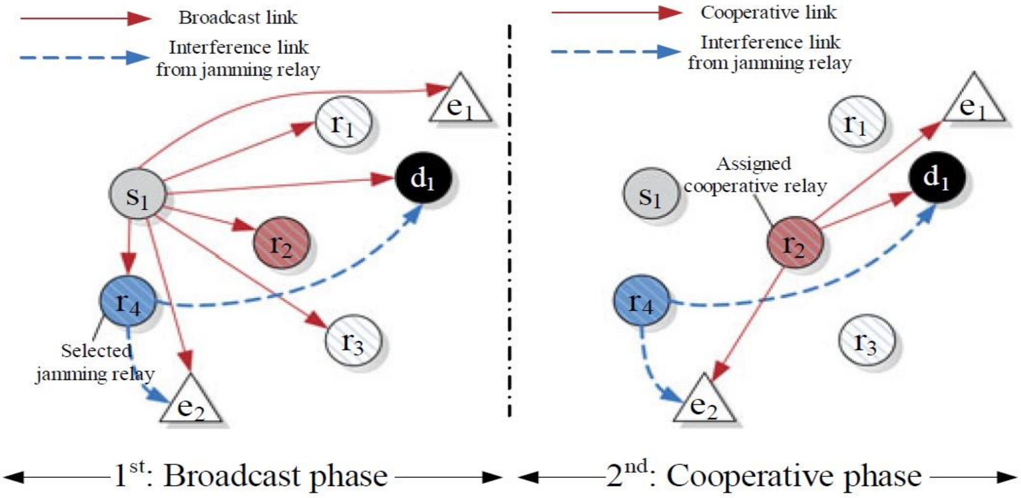


Fig. 1: Cooperative communication phases with a selected friendly jammer

V. PERFORMANCE EVALUATION

Simulation Results

Simulation is performed using NS-2 tool for the proposed algorithm in the DSDV protocol. The performance metrics such as end to end delay, packet delivery ratio, throughput and overhead are analyzed and obtained. The simulation parameters are tabulated.

Table 6.1 Simulation Parameters

Simulation Time	20 Minutes
Number of nodes	50
Node replacement strategy	Random
Propogation Model	Two ray model
Mobility model	Random way point
Network protocol	MAC/802.11
Routing Protocol	DSDV

DSDV Protocol

Destination sequenced distance vector routing (DSDV) is adapted from the conventional Routing Information Protocol (RIP) to ad hoc networks routing. It adds a new attribute, sequence number, to each route table entry of the conventional RIP. Using the newly added sequence number, the mobile nodes can distinguish stale route information from the new and thus prevent the formation of routing loops.

Packet Routing and Routing Table Management

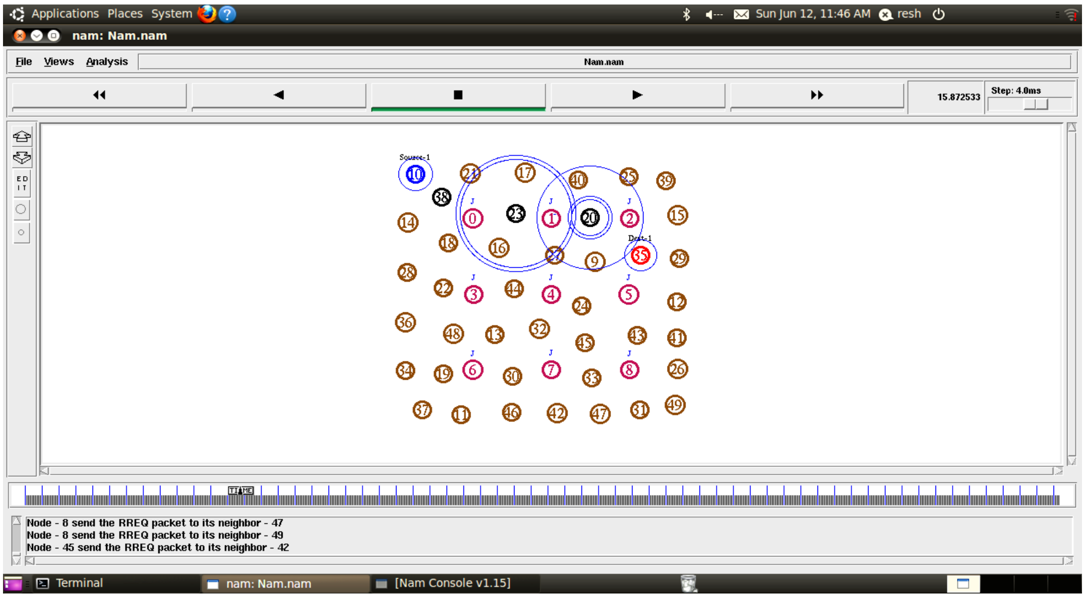
In DSDV, each mobile node of an ad hoc network maintains a routing table, which lists all available destinations, the metric and next hop to each destination and a sequence number generated by the destination node. Using such routing table stored in each mobile node, the packets are transmitted between the nodes of an ad hoc network. Each node of the ad hoc network updates the routing table with advertisement periodically or when significant new information is available to maintain the consistency of the routing table with the dynamically changing topology of the ad hoc network. Periodically or immediately when network topology changes are detected, each mobile node advertises routing information using broadcasting or multicasting a routing table update packet. The update packet starts out with a metric of one to direct connected nodes. This indicates that each receiving neighbour is one metric (hop) away from the node. It is different from that of the conventional routing algorithms. After receiving the update packet, the neighbours update their routing table with incrementing the metric by one and retransmit the update packet to the corresponding neighbours of each of them. The process will be repeated until all the nodes in the ad hoc network have received a copy of the update packet with a corresponding metric. The update data is also kept for a while to wait for the arrival of the best route for each particular destination node in each node before updating its routing table and retransmitting the update packet. If a node receives multiple update packets for a same destination during the waiting time period, the routes with more recent sequence numbers are always preferred as the basis for packet forwarding decisions, but the routing information is not necessarily advertised immediately, if only the sequence numbers have been changed. If the update packets have the same sequence number with the same node, the update packet with the smallest metric will be used and the existing route will be discarded or stored as a less preferable route. In this case, the update packet will be propagated with the sequence number to all mobile nodes in the ad hoc network. The advertisements of routes that are about to change may be delayed until the best routes have been found. Delaying the advertisement of possibly unstable route can damp the fluctuations of the routing table and reduce the number of rebroadcasts of possible route entries that arrive with the same sequence number. The elements in the routing table of each mobile node change dynamically to keep consistency with dynamically changing topology of an ad hoc network. To reach this consistency, the routing information advertisement must be frequent or quick enough to ensure that each mobile node can almost always locate all the other mobile nodes in the dynamic ad hoc network. Upon the updated routing information, each node has to relay data packet to other nodes upon request in the dynamically created ad hoc network.

Throughput

The number of attackers is increased in each stage and the throughput and delay are analysed. Throughput is calculated as the ratio of the output in bits to the difference in time of the first packet sent and the last packet received. It is measured in bits per second.

Packet Delivery Ratio

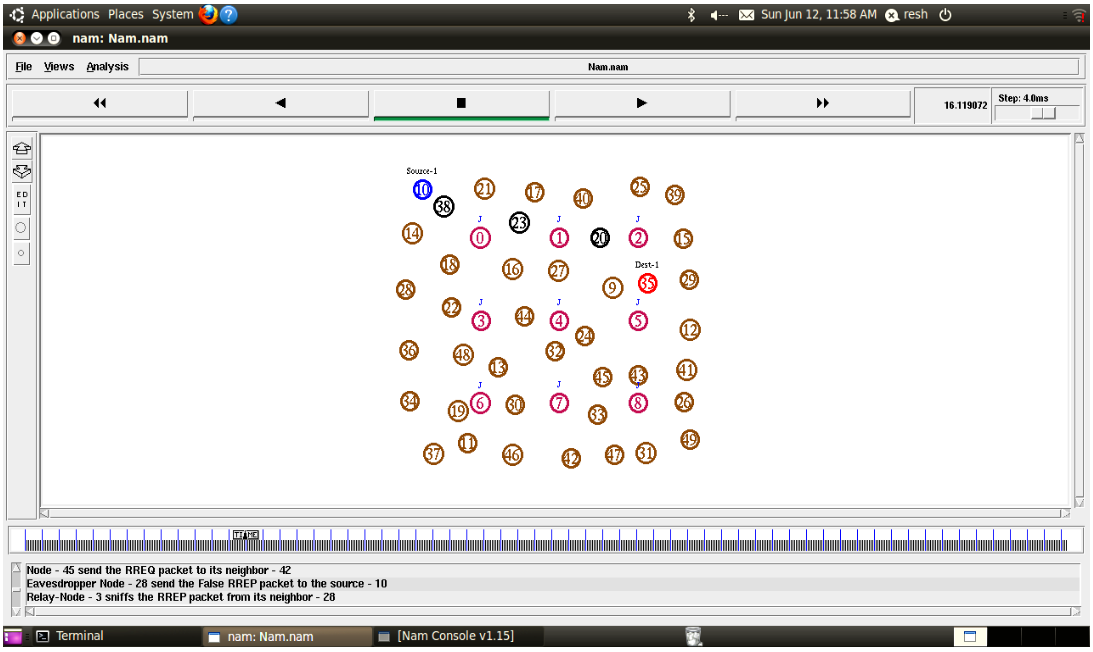
Packet delivery ratio is defined as the ratio number of packets received to the number of packets sent.



```
Node - 8 send the RREQ packet to its neighbor - 47
Node - 8 send the RREQ packet to its neighbor - 49
Node - 45 send the RREQ packet to its neighbor - 42
```

Fig.2 Transmission between source1 and destination1

The above fig.2 shows the transmission1 between source1 (10) and destination1 (35). Nodes38,23,20 are selected as relay node due to large transmission range between source and destination node.



```
Node - 45 send the RREQ packet to its neighbor - 42
Eavesdropper Node - 28 send the False RREP packet to the source - 10
Relay-Node - 3 sniffs the RREP packet from its neighbor - 28
```

Fig. 3 Eavesdropper node detection

The above fig. 3 shows the detection of eavesdropper node. Node 28 sends false RREP packet to the source node 10. But node 28 is not a selected relay node. So jamming node 3 detects node 28 as malicious node and mark that in the block table.

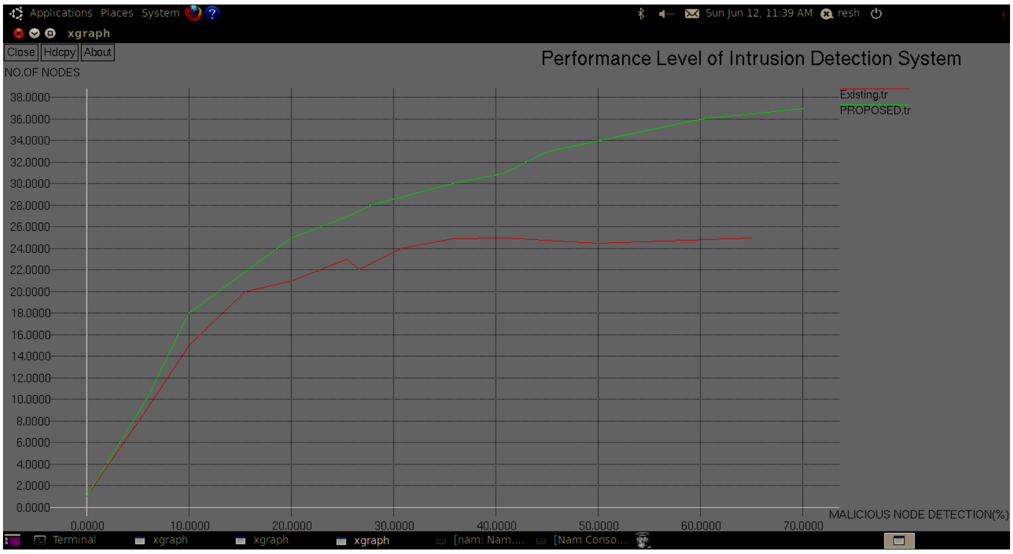


Fig.4 Performance level of intrusion detection system

The above fig.4 shows the performance level of intrusion detection system. X-axis represents the time scale of Malicious node detection in percentage and Y-axis represents the No. of nodes. The graph shows comparison between existing and proposed system. Detection of malicious nodes increases in proposed system due to use of cryptography mechanism.

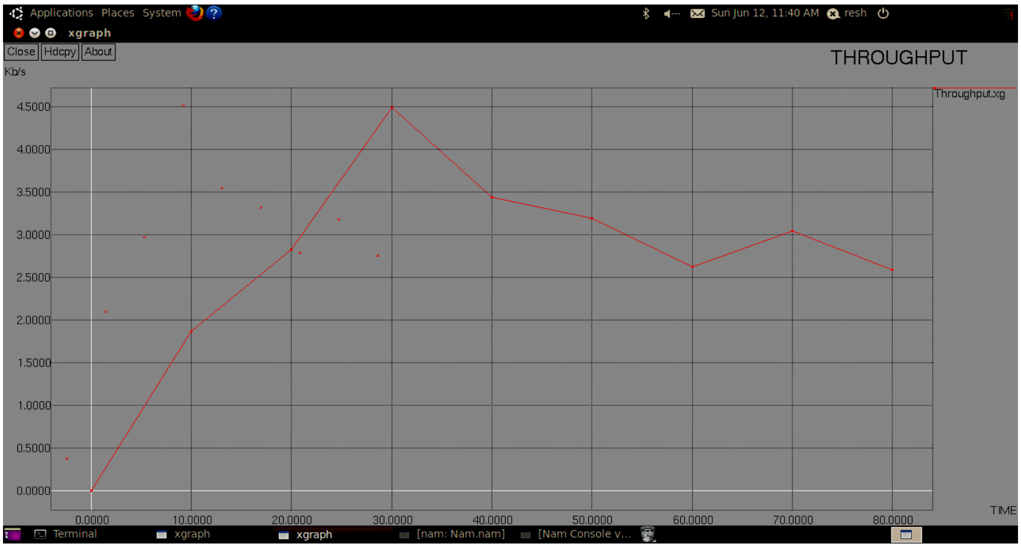


Fig.5 Throughput graph

The above fig.5 shows the throughput graph for the proposed system. X-axis represents the time and Y-axis represents the speed in Kb/s.

V. CONCLUSION

With the advancement of telecommunication technology, devices with wireless functionalities are ubiquitous nowadays. As a result, networking among such devices has become increasingly critical in both theory and practice. By using IBS scheme we can provide a proper authentication mechanism in order to avoid the malicious node involvement in the packet transmission. With the help RREP and RREQ process we can detect the malicious node involved in the transmission. By using relay nodes we can make the transmission more successful if the transmission range is high. Further use of jamming algorithm, we can further increase the secrecy capacity and make a friendly jammer towards the malicious node and prevent the malicious node from the further transmission. The final graphs shows the throughput and performance automatically improved compared to the existing techniques because here we used the combined cryptography and smart jamming for more secrecy.

REFERENCES

[1] Huang Lu, Student Member, IEEE, Jie Li, Senior Member, IEEE, and Mohsen Guizani, Fellow, IEEE- 'Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks'.

[2] AggelosBletsas, Member, IEEE, Hyundong Shin, Member, IEEE, and Moe Z. Win, Fellow, IEEE(2007)' Cooperative Communications with Outage-Optimal Opportunistic Relaying'.

[3] Biao Han, Member, IEEE, Jie Li, Senior Member, IEEE, Jinshu Su, Member, IEEE, MinyiGuo, Senior Member, IEEE, and Baokang Zhao, Member, IEEE(2015)-' Secrecy Capacity Optimization via Cooperative Relaying and Jamming for WANETs'.

[4] Edna Elizabeth N., Subasree S., S. Radha WSEAS TRANSACTIONS on COMMUNICATIONS-'Enhanced Security Key Management Scheme for MANETS'

[5] Q.Wang, H. Su, K. Ren, and K. Kim(2011), "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in Proc. IEEE Conf. Comput. Commun.

[6] S. K. LEUNG-YAN-CHEONG, MEMBER, IEEE, AND MARTIN E. HELLMAN, MEMBER, IEEE(1978)- The Gaussian Wire-Tap Channel.

[7] Sushant Sharma, Student Member, IEEE, Yi Shi, Member, IEEE, Y. Thomas Hou, Senior Member, IEEE, and SastryKompella, Member, IEEE(2011)-' An Optimal Algorithm for Relay Node Assignment in Cooperative Ad Hoc Networks'.

[8] Tairan Wang, Student Member, IEEE, and Georgios B. Giannakis, Fellow, IEEE(2008) 'Mutual Information Jammer-Relay Games.'

[9] X. Shen, A. Hjrungnes, Q. Zhang, P. R. Kumar, and Z. Han(Feb. 2012) "Guest editorial: Cooperative networking - challenges and applications (Part 1)," IEEE J. Sel. Areas Commun.