ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com
International Journal of Advanced Research Trends in Engineering and ıology (IJARTET)
Vol. 5, Special Issue 12, April 2018

EFFICEINT TRUST MODEL WITH AN EFFECTIVE DEFENCE SCHEME IN MANETs FOR MILITARY APPLICATIONS

M. Tamil Selvi [1], Dr.V.Selvi [2]
[1]*M.phil Scholar, Departmetn of Computer Science, Mother Teresa Women's University, Kodaikanal*
[2]*Assistant Professor, Dept of Computer Science, Mother Teresa Women's University, Kodaikanal*
tamilmca.selvi7@gmail.com

Abstract— — — The reliability of delivering packets through multi-hop intermediate nodes is a significant issue in the mobile ad hoc networks (MANETs). The distributed mobile nodes establish connections to form the MANET, which may include selfish and misbehaving nodes. Recommendation based trust management has been proposed in the literature as a mechanism to filter out the misbehaving nodes while searching for a packet delivery route. However, building a trust model that adopts recommendations by other nodes in the network is a challenging problem due to the risk of dishonest recommendations like bad-mouthing, ballot-stuffing, and collusion. Proposed system investigate the problems related to attacks posed by misbehaving nodes while propagating recommendations in the existing trust models. Proposed a recommendation based trust model with a defense scheme, which utilizes clustering technique to dynamically filter out attacks related to dishonest recommendations between certain time based on number of interactions, compatibility of information and closeness between the nodes. We evaluate the trust degree as two cases like direct and indirect trust values between neiboring nodes from source. To form an clustering routing network from similar trust values from S to D. The model is empirically tested under several mobile and disconnected topologies in which nodes experience changes in their neighborhood leading to frequent route changes. The empirical analysis demonstrates robustness and accuracy of the trust model in a dynamic MANET environment.

Keywords – MANET, trust, topologies, model

I INTRODUCTION

A wireless sensor network is a spatially distributed autonomous sensors networks to monitor physical and environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the networks to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance, today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts, a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created

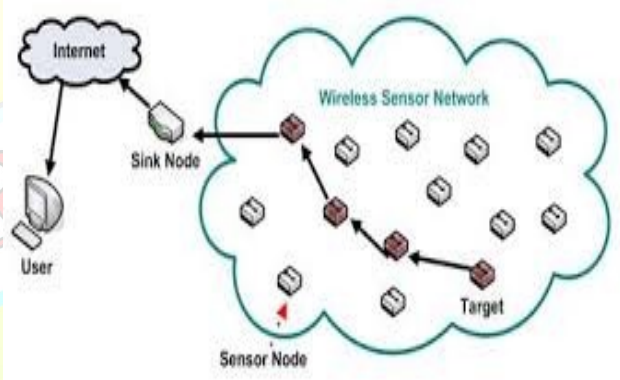

Fig:1 Architecture of WSNs

Wireless Sensor Networks (WSN), sometimes called Wireless sensor network and actuator networks are spatially distributed autonomous sensor to monitor physical or environment conditions, such as temperature, sound, pressure etc. and to cooperatively pass their data through the network to other locations. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes.

A mobile ad hoc network (MANET), also known as wireless ad hoc network or ad hoc wireless network is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com
International Journal of Advanced Research Trends in Engineering and ıology (IJARTET)
Vol. 5, Special Issue 12, April 2018

Managing trust in a distributed mobile ad hoc network (MANET) is a challenging when collaboration or cooperation is critical to achieving mission and system goals such as reliability, availability, scalability, and reconfigurablity. In defining and managing trust in a military MANET, we must consider the interactions between the composite cognitive, social information and communication networks, and take into account the severe resource constraints (eg.., computing power, energy, bandwidth, time), and dynamics (eg.topology changes, node mobility, node failure, propagation channel conditions).

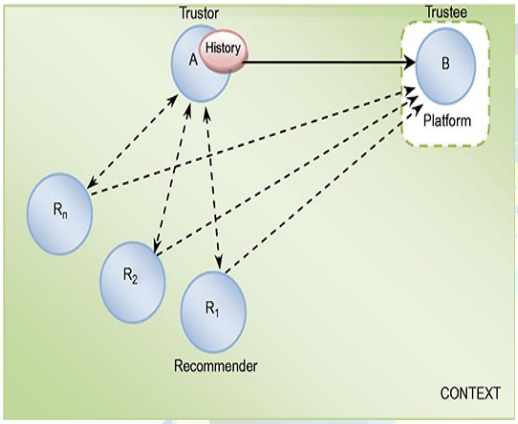

Fig 2: Trust Management in WSNs

In an on-demand routing protocol, the source node floods the Route Request packet in the network when a route is not available for the desired destination. It may obtain multiple routes to different destinations from a single Route Request. The major difference between AODV and other on-demand routing protocols is that it uses a destination sequence number (DestSeqNum) to determine an up-to-date path to the destination. A node updates its path information only if the DestSeqNum of the current packet received is greater or equal than the last DestSeqNum stored at the node with smaller hop count.

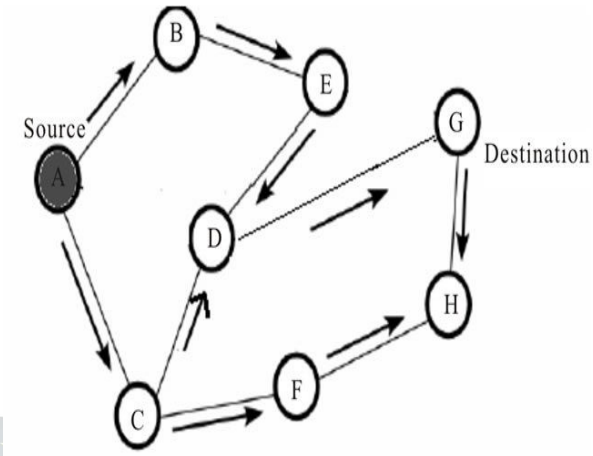

Fig: 3 Source Sending a Route Request Packet

II RELATED WORK

Ing-Ray Chen, FenyeBao, MoonJeong Chang, and Jin-Hee Cho "Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing" IEEE Transactions on Parallel and Distributed Systems, May2013.

Delay tolerant networks (DTNs) are characterized by high end-to-end latency, frequent disconnection, and opportunistic communication over unreliable wireless links. In this paper, we design and validate a dynamic trust management protocol for secure routing optimization in DTN environments in the presence of well-behaved, selfish and malicious nodes. We develop a novel model-based methodology for the analysis of our trust protocol and validate it via extensive simulation. Moreover, we address dynamic trust management, i.e., determining and applying the best operational settings at runtime in response to dynamically changing network conditions to minimize trust bias and to maximize the routing application performance. We perform a comparative analysis of our proposed routing protocol against Bayesian trust-based and non-trust based (PROPHET and epidemic) routing protocols. The results demonstrate that our protocol is able to deal with selfish behaviors and is resilient against trust-related attacks. Furthermore, our trust-based routing protocol can effectively trade off message overhead and message delay for a significant gain in delivery ratio. Our trust-based routing protocol operating under identified best settings outperforms Bayesian trust-based routing and PROPHET, and approaches the ideal performance of epidemic routing in delivery ratio and message delay without incurring high message or protocol maintenance overhead.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com
International Journal of Advanced Research Trends in Engineering and ıology (IJARTET)
Vol. 5, Special Issue 12, April 2018

"Self-Adaptive On-Demand Geographic Routing for Mobile Ad Hoc Networks" Xiaojing Xiang, Member, IEEE, Xin Wang, Member, IEEE, and Zehua Zhou, Member, IEEE, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 11, NO. 9, SEPTEMBER 2012

It has been a big challenge to develop a routing protocol that can meet different application needs and optimize routing paths according to the topology changes in mobile ad hoc networks. Basing their forwarding decisions only on local topology, geo graphic routing protocols have drawn a lot of attentions in recent years. However, there is a lack of holistic design for geographic routing to be more efficient and robust in a dynamic environment. Inaccurate local and destination position information can lead to in efficient geographic forwarding and even routing failure. The use of proactive fixed-interval beaconing to distribute local positions introduces high overhead when there is no traffic and cannot capture the topology changes under high mobility. It is also difficult to preset protocol parameters correctly to fit in different environments. In this work, we propose two self-adaptive on-demand geographic routing schemes which build efficient paths based on the need of user applications and adapt to various scenarios to provide efficient and reliable routing. To alleviate the impact due to inaccurate local topology knowledge, the topology information is updated at a node in a timely manner according to network dynamics and traffic demand. On-demand routing mechanism in both protocols reduces control overhead compared to the proactive schemes which are normally adopted in current geographic routing protocols. Additionally, our route optimization scheme adapts the routing path according to both topology changes and actual data traffic requirements .Furthermore, adaptive parameter setting scheme is introduced to allow each node to determine and adjust the protocol parameter values independently according to different network environments, data traffic conditions, and node's own conditions. Our simulation studies demonstrate that the proposed routing protocols are more robust and outperform the existing geographic routing protocol and conventional on-demand routing protocols under various conditions including different mobilities, node densities, traffic loads, and destination position inaccuracies. Specifically, the proposed protocols could reduce the packet delivery latency up to 80 percent as compared to GPSR at high mobility. Both routing protocols could achieve about 98 percent delivery ratios, avoid incurring unnecessary control overhead, have very low forwarding overhead and transmission delay in all test scenarios.

MoazamBidaki and Mohammad Masdari "Reputation-Based Clustering Algorithms in Mobile Ad Hoc Networks"International Journal of Advanced Science and Technology Vol. 54, May, 2013

Clustering is one of the main techniques that are used to increase the scalability of MANETs, but without any security considerations clustering is prone to various security attacks. Some cryptographic-based schemes have been proposed to secure the clustering process, but they are unable to handle the internal attacks. Trust-based clustering schemes have combined the trust management systems with the existing state of art clustering solutions and using cryptographic mechanism these schemes present the most complex and secure clustering solutions that are resilient against both internal and external attackers. In this paper, we present an in-depth analysis of trust-based clustering schemes and illustrate how reputations are integrated in these schemes. Then we compare them based on the various trust metrics and finally conclude with open research issues.

Security and Privacy are most vital matters in Vehicular Ad-hoc Networks (VANET). Usage of pseudonyms is the extensively approved privacy preserving communication method in VANET. Pseudonyms have provided great solutions for security problems like Sybil attack. Reza Mortazavi Maryam Rahbari (2011) designed an efficient method to detect Sybil attack during the privacy preserving of vehicles in the network. Distributed and hierarchical method has also been developed that meets all security requirements of VANET. The proposed method is more efficient and robust against probable attacks when compared with other similar methods. The number of attackers has got much more limited, and a global privacy attack is approximately infeasible. Privacy-preserving methods in VANET are mostly susceptible to Sybil attacks, where a malicious user can act as if a multiple (other) vehicle.

Tong Zhou et al (2011) proposed a lightweight and scalable protocol called Privacy Preserving Detection of Abuses of Pseudonyms (P2DAP) to identify Sybil attacks. In the proposed protocol a malicious user acts as multiple (other) vehicle is detected in a distributed manner by the help of passive overhearing by a group of fixed nodes denoted as road-side boxes (RSBs). The discovery of Sybil attacks by the above mentioned form does not necessitate any vehicle in the network to reveal its identity by which privacy is safeguarded at all times. The downside in P2DAP is that the ratio and activities of mischievous vehicles are not predicted; hence for that a machine learning algorithm has to be developed. If the attackers are found, then P2DAP can identify attackers with more minimized overhead and delay. Besides the security and privacy in VANET, usage of Nash equilibrium is most important as it provides an efficient VANET. Gireesh Shrimali et al (2010) proposed a novel method for inter domain traffic

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com
International Journal of Advanced Research Trends in Engineering and ıology (IJARTET)
Vol. 5, Special Issue 12, April 2018

engineering and it depends on Nash bargaining and dual decomposition.

The Nash product is a social cost function and it is enhanced by ISPs which use an iterative method. The global optimization problem is partitioned into sub problems by offering suitable shadow prices on the inter domain flows. The sub problems are then solved separately in a distributed form by the individual ISPs. The proposed method considerably outperforms than the commonly used hot-potato or shortest path routing as well as the Nash equilibrium setting. Nash equilibrium routing takes active load-based costs on the links rather than the static weight-based optimization of the hot-potato routing. The Nash equilibrium routing is an active method; it takes numerous iterations to converge which is the drawback. The above said problem can be solved by the usage of centrality measures but there is no guarantee for good result. Vehicular network is a simpler network and needs more secured transmission. TansuAlpcan& Sonja Buchegger (2011) proposed an upgraded transportation security, reliability, and management in vehicular networks (VANETs). A game-theoretic framework is employed and by which the security approach of VANETs is measured.

III PROBLEM FORMULATION

A sender will consider an interaction as successful if the sender receives an assurance that the packet is successfully received by the neighbor node and that node has forwarded the packet toward the destination in an unaltered fashion. Thus the first requirement, i.e., successful reception, is achieved on reception of the link layer acknowledgment (ACK). IEEE 802.11 is a standard link layer protocol, which keeps packets in its cache until the sender receives an ACK. Whenever the receiver node successfully received the packet; it will send back an ACK to the sender. If the sender node did not receive the ACK during a predefined threshold time, then it will retransmit that packet.

IV PROPOSED WORK IMPLEMENTATION

REPRESENTATION OF TRUST VALUE

Generally, a trust value is considered to be a numerical quantity lying between 0 and 1 (inclusive) or between _1 and 1 (inclusive) on a real number line. In this paper, we use trust value as an integer in the interval between 0 and 100 (inclusive). However, other ranges, for example base 2 ranges, could be used as well. Although presenting the trust values as a real number or integer may not play an important role in traditional networks, but for SNs this issue is of critical importance due to limited memory, and transmission, reception power. This change will give us benefits such as:

Representation of trust value [0, 100] as an unsigned integer (1 byte) saves 75 percent of memory space as compared to trust values represented as a real number (4 bytes). Less number of bits needs to be transmitted during the exchange of trust values between SNs. This gives us the benefit of less consumption of transmission and reception power.

ASSUMPTIONS

We assume that the sensor network consists of large number of SNs that are deployed in an open or hostile environment. We also assume that all SNs have unique identities. In some of the sensor network models, nodes do not have unique identities like IP in traditional networks. However, in order to uniquely identify the SNs and perform communication in those environments, class-based addressing scheme is used, in which a node is identified by a tripletlocation, node type, node subtype. We also, assume that SNs are organized into clusters with the help of any proposed clustering scheme. We also assume that the BS is a central command authority. It has no resource constraint problem, and furthermore, it cannot be compromised by an attacker. In order to provide protection of trust values from traffic analysis or fabrication during transfer from one node to another, we assume a secure communication channel, which can be established with the help of any key management scheme.

GROUP-BASED TRUST MANAGEMENT SCHEME

The proposed trust model works with two topologies. One is the intra group topology where distributed trust management is used. The other is intergroup topology where centralized trust management approach is employed. For the intra group network, each sensor that is a member of the group calculates individual trust values for all group members. Based on the trust values, a node assigns one of the three possible states: 1) trusted, 2) untrusted, or 3) uncertain to other member nodes. This three-state solution is chosen for mathematical simplicity and is found to provide appropriate granularity to cover the situation. After that, each node forwards the trust state of all the group member nodes to the CH. Then, centralized trust management takes over. Based on the trust states of all group members, a CH detects the malicious

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com
International Journal of Advanced Research Trends in Engineering and ıology (IJARTET)
Vol. 5, Special Issue 12, April 2018

node(s) and forwards a report to the BS. On request, each CH also sends trust values of other CHs to the BS. Once this information reaches the BS, it assigns one of the three possible states to the whole group. On request, the BS will forward the current state of a specific group to the CHs. Our group-based trust model works in three phases: 1) Trust calculation at the node level, 2) trust calculation at the cluster-head level, and 3) trust calculation at the BS level.

TRUST CALCULATION AT THE CLUSTER-HEAD LEVEL

Here, we assume that the CH is the SN that has higher computational power and memory as compared to other SNs.

Trust State Calculation of Intra Group

In order to calculate the global trust value of nodes in a group, CH asks the nodes for their trust states of other members in the group. We use the trust states instead of the exact trust values due to two reasons. First, the communication overhead would be less as only a simple state is to be forwarded to the CH. Second, the trust boundaries of an individual node vary from other nodes. A particular trust value might be in a trusted zone for one node, whereas it may only correspond to the uncertain zone for another node. Hence, the calculation of the global trust state of nodes in a group would be more feasible and efficient if we only calculate it using the trust states. Let us suppose there are n þ 1 nodes in the group including the CH. The CH will periodically broadcast the request packet within the group. In response, all group member nodes forward their trust states, s, of other member nodes to the CH. The variable, s, can take three possible states: trusted, uncertain, and untrusted. The CH will maintain these trust states in a matrix form, as shown below

$$T\,Mch = \begin{matrix} sch,1 & s1,c & \dots sn,1 \\ sch,2 & s1,2 & \dots sn,2 \\ \vdots & \vdots & \vdots \end{matrix}$$

Where TMch represents the trust state matrix of cluster head ch, and sch;1 represents the state of node 1 at cluster head ch. The CH assigns a global trust state to a node based on the relative difference in trust states for that node. We emulate this relative difference through a standard normal distribution. Therefore, the CH will define a random variable X such that

$$\text{Trust value of the node} = \begin{cases} 2, & \text{when trusted} \\ 1, & \text{when uncertain} \\ 0, & \text{when untrusted} \end{cases}$$

Assuming this to be a uniform random variable, we define the sum of m such random variables as Sm. The behavior of Sm will be that of a normal variable due to the central limit theorem. The expected value of this random variable is m and the standard deviation $\sqrt{m/3}$.The CH defines the following standard normal random variable for a node j,

$$Z_j = \frac{\sqrt{3\left(X(S_{ch,j}) + \sum_{i=1,i\neq j}^{m} X(S_{ch,j}) - m\right)}}{\sqrt{m}}$$

If $Z_j \epsilon$ [-1, 1], then node j is termed as uncertain, else if $Z_j > 1$, it is called trusted. If $Z_j < -1$, it is labeled as un trusted.

To dynamically select the cluster head based on the energy profile of each node and to implement secure routing by incorporating group based trust management schemes in a wireless sensor network. The simulated output is compared with the existing dynamic trust management scheme with the parameters of energy dissipation, consumption and packet delivery ratio.

FLOW STRUCTURE

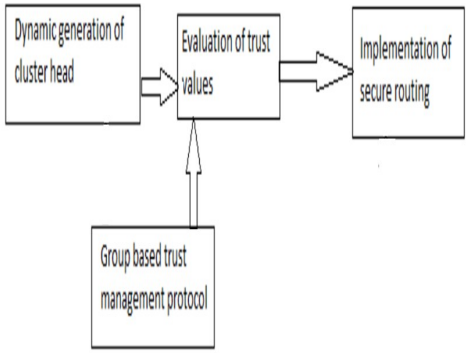

Fig 4 Structure of programming for proposed work

EXPLANATION

Our approach is to dynamically create the cluster heads based on energy profile on each and every node and to validate a Group-Based trust management scheme for secure routing for optimization in sensor networks. The simulation results show that our scheme demands less energy consumption and energy dissipation as compared with the dynamic trust-based management schemes and it is secure for routing in wireless sensor networks.

The wireless sensor network with 50 nodes is created in the NS-2.34 version. An energy model is used to calculate the energy of each node. Now the energy calculated for the nodes is compared with one another and the node with higher energy is found. This node with higher node energy is assumed as the cluster head. As a next step the trust values of

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com
International Journal of Advanced Research Trends in Engineering and nology (IJARTET)
Vol. 5, Special Issue 12, April 2018

the 50 nodes are calculated considering the successful and unsuccessful transmissions. If the trust value of the node is 2 then the node is trusted node. If the trust value is other than 2 then the nodes are considered untrusted according to the Group based trust management scheme .Now the trusted nodes are found and their node color is changed. After finding the trusted nodes the transmission between the trusted nodes occurs and finally the packets are transmitted to the cluster head. If there is any transmission between untrusted then there is some packet drop. Finally we draw X-graph and Gnu plot for the required parameters.

VI. EXPERIMENTAL RESULTS

Simulation software	NS-2
Monitoring area	1500 X 1500 m^2
Number of nodes	50
Routing protocol	AODV
MAC type	Mac 802_11
Number of packets	200
Antenna model	Omni directional
Initial energy value	100
Interface queue type	DropTail queue
Propagation model	Two ray model

Table 1: simulation parameters

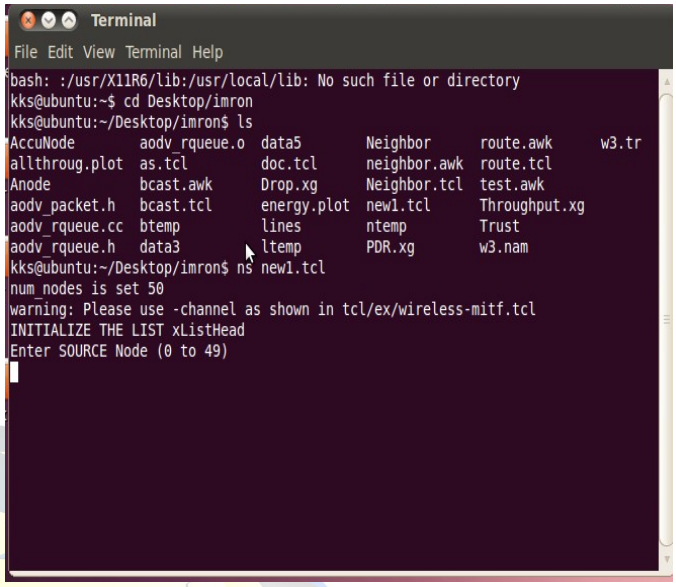

Fig 5 Terminal window

In the simulation window, fifty nodes are created. The cluster head is assigned dynamically by calculating the energy of each node. The trust values of the nodes are checked and the trusted nodes are identified. Then routing in intra group is done via trusted nodes to cluster head.

The screen shots are taken while running the program in ns2.

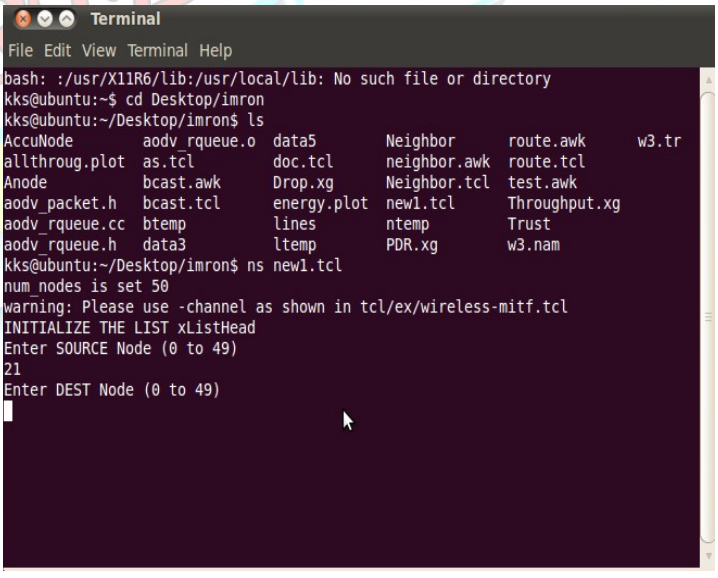

Fig: 6 Source node selections

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com
International Journal of Advanced Research Trends in Engineering and
nology (IJARTET)
Vol. 5, Special Issue 12, April 2018

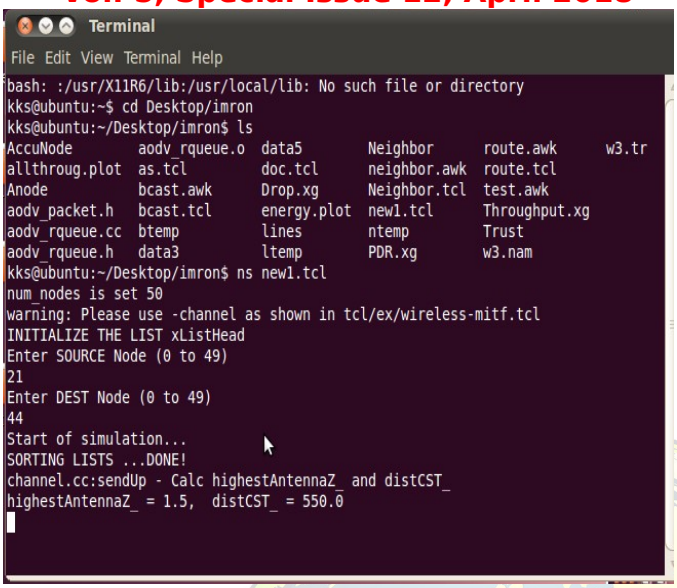

Fig:7 Destination Source selection

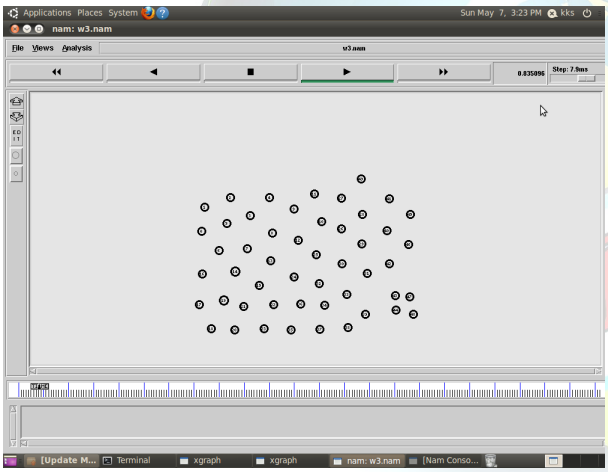

Fig 8 Formation of nodes

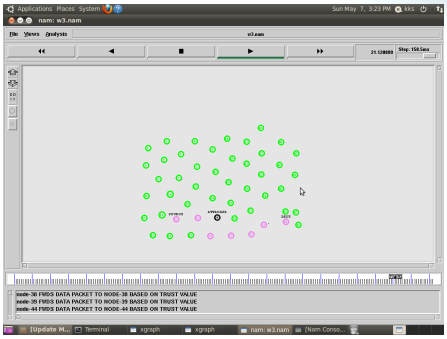

Fig: 9 secure routing with attacker detection with trusted nodes

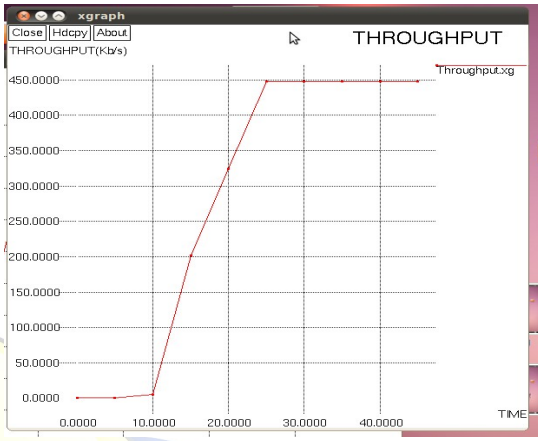

Fig: 10 Proposed throughput graph

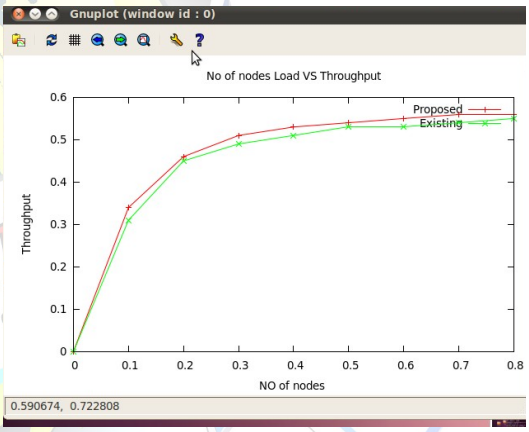

Fig: 11 comparison graph throughput

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com
International Journal of Advanced Research Trends in Engineering and ıology (IJARTET)
Vol. 5, Special Issue 12, April 2018

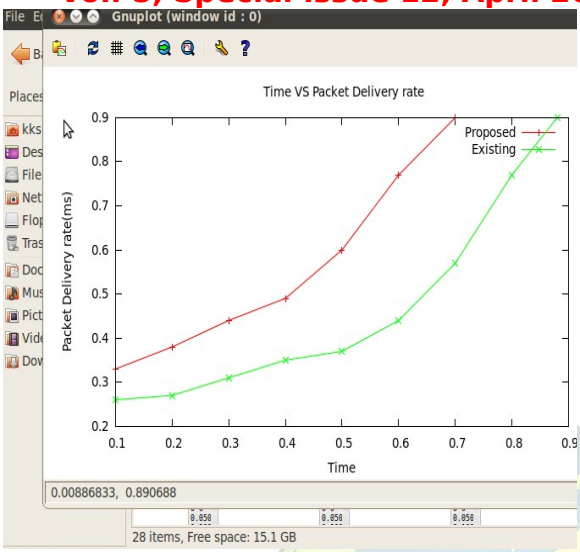

Fig: 12 comparison graph with PDR

CONCLUSION

Main objective is to implement the secure routing in MANET from the energy profile which is defined and the energy of the node is given in the terminal after running the code. Using the function Energy Model function the energy of the nodes are calculated. The group based trust management scheme is validated and trust values of the trusted nodes are calculated and displayed in the terminal and secure routing is done via trusted nodes using trust table which is defined with routing table for secure routing optimization in Mobile adhoc network.

In Future work dynamic cluster based network considered for complex computation to determine the energy efficient routing from S to D

REFERENCES

[1] I. R. Chen, F. Bao, M. Chang, and J. H. Cho, "Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing",IEEE Transactions on Parallel and Distributed Systems, 2013.

[2] R.A.Shaikh, Hassan Jameel, BrianJ.d'Auriol, "Group-based trust management scheme for clustered wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 11, pp. 1698–1712, Nov. 2009.

[3] MoazamBidaki and Mohammad Masdari, "Reputation-Based Clustering Algorithms in Mobile Ad Hoc Networks", International Journal of Advanced Science and Technology Vol. 54, May, 2013.

[4] K.Liu, N.Abu-Ghazaleh, and K.-D. Kang, "Location Verification and Trust Management for Resilient Geographic Routing," Parallel and Distributed Computing, vol. 67, no. 2, pp. 215-228, 2007.

[5] Shaila K, S H Manjula, Venugopal K R and L M Patnaik**, "**Anonymity Trust Management Scheme (ATMS) for Clustered Wireless Sensor Networks", International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 8, Number 2 (2012), pp. 133-153.

[6] Mohammad Sadeghi, FarshadKhosravi, KayvanAtefi, Mehdi Barati, "Security Analysis of Routing Protocols in Wireless Sensor Networks",IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3, January 2012,ISSN (Online): 1694-0814.

[7] A. Vinel, "Performance aspects of vehicular ad-hoc networks: Current research and possible trends," presented at the GI/ITGWorkshopMMBnet, Hamburg, Germany, Sep. 2009.

[8] R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, "Toward cloudbased vehicular networks with efficient resource management,"IEEENetw. Mag., vol. 27, no. 5, pp. 48–54, Sep./Oct. 2013.

[9] K. Yang, S. Ou, H. Chen, and J.He, "A multihop peer-communicationprotocol with fairness guarantee for IEEE 802.16-based vehicularnetworks," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3358–3370, Nov. 2007.

[10] Z. Wang and J. Crowcroft, "Quality-of-service routing for supporting multimedia applications," IEEE J. Select. Areas Comm. vol. 14, no. 7, pp. 1228–1234, Sep. 1996.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com
International Journal of Advanced Research Trends in Engineering and nology (IJARTET)
Vol. 5, Special Issue 12, April 2018

[11] D. S. Reeves and H. F. Salama, "A distributed algorithm for delay constrained unicast routing," IEEE/ACM Trans. Netw., vol. 8, no. 2, pp. 239–250, Apr. 2000.