International Journal of Scientific Research in Computer Science, Engineering and Information Technology

© 2018 IJSRCSEIT | Volume 3 | Issue 8 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT183839

Reduction of Malicious Nodes using RRT and Clustering in Mobile Ad hoc Network

Zulfekar Ahmad, Akhilesh Bansiya

Computer Science and Engineering, Vedica Institute of Technology, Bhopal, Madhya Pradesh, India

ABSTRACT

Mobile Ad-hoc Network is a collection of wireless mobile node, consists of each wireless transmitters and receivers, which dynamically forming a temporary network and communication between transmitter and receiver is by using bi-directional link. Either directly, if nodes in MANET are within communication range or indirectly means transmitter node rely on intermediate node, for forwarding data to destination node. IDS can be well-defined as the protector system which self-detects malicious activities within a network, and thus generates an alarm to alert the security device at a locality if intrusions are considered to be illegal on that network or host. There me many approach to classify IDS. In the existing work, they used fuzzy logic which decides the rules for the trust evaluation of the nodes. Rules should be defined previously which is difficult to manage for the unknown variables. This method is not suitable for the dynamic nature of the network. So we applied better technique which generates the more trustful network. In our proposed work, trust is calculated by sending the Route Request (RREQ) packets to the network then the destination node send Route Reply (RREP) packet. Calculate RTT for distance between the sender and destination nodes. We select the path by taking the shortest RTT and then form clusters. Calculate the energy of each node in cluster and select cluster head of maximum energy. Cluster head forward the data from source to destination. This method removes the chance of malicious node from the network.

Keywords : MANET, IDS, RREQ, RTT, RREP, fuzzy logic , Large Mobile Host, DBMS

I. INTRODUCTION

MANET is the wirelessly ad hoc network in which every tool is loose to transport freely in any path. MANET is the self-configuring and infrastructure-much less networks aiming to support mobility of devices. Each device changes its hyperlinks to other devices often ensuing in a incredibly dynamic and autonomous topology. An IDS is a programming or device application which framework exercises for produces reports and strategy infringement to an administration station. Intrusion is any arrangement of activities that endeavor to involve the respectability, secrecy or accessibility and IDS is a gadget or software application that observers network traffic movement and if any suspicious action discovered then it cautions the system or network overseer. There are three main modules of IDS are Monitoring, Analyses, Response. To beat this issue, intrusion-detection system (IDS) ought to be added to upgrade the security level of MANETs. On the off chance that MANET knows how to the distinguish the assailants when they enters in the system, we will ready to totally evacuate the potential harms brought about by traded off nodes at the first run through. IDS generally go about as the second layers in MANETs.

MANETs likened to other network suffer from certain grave disadvantages. The nonexistence of any fixed infrastructure accessible is a more significant. Cause of these ad-hoc networks is best suited in circumstances where the infrastructure is either unavailable or not trusted for example military scenarios. Cause of this the security aspect becomes one of the most important and nontrivial aspects. So, the object of the thesis is to make a methodology for examining MANET, both hostile and non-hostile environment. Also there is a focus on abridging the simulating process in other to allow gathering signatures for distributed IDS scheme. Following objectives are realized to attain the goal:

- Review of ad-hoc networks modelling approach
- Review of IDS system proposed for MANET
- Analyze of the simulation process and present possible improvements
- Perform experiments in sequence to evaluate existing methods
- Evaluation of gathered information.

II. METHODS AND MATERIAL

Mobile Ad Hoc Network

Wireless networking is the platform for working with the cutting- technology extensively used in several programs. Mobile Ad-hoc Network is a collection of wireless mobile node, comprise of all wirelessly sender and destination that dynamically forming a temporary network and communiqué amid transmitter and receiver is thru utilizing bi-directional link. Either directly, if nodes in MANET are within communication range or indirectly means transmitter node rely on intermediate node, for forwarding data to destination node. Various feature of MANET, overcomes the problem in contemporary application of wireless network. for example, dynamic topology and decentralized network highlight of MANET, means every one of the nodes are allowed to move haphazardly. The self-arranging capacity of nodes in MANET, Minimal arrangement and snappy improvement, makes MANET prepared to be utilized as a part of crisis condition, where a foundation is inaccessible, or hard to introduce organize, in situations like catastrophic events, military clashes. Because of these different one of a kind qualities,

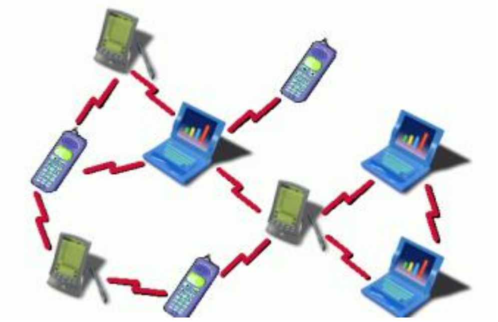

Figure1 : Wirelesses MANET

Advantages of MANET

- They give access to data and administrations paying little respect to geographic position.
- Independence from focal network organization. Self-designing network, nodes are likewise go about as switches. More affordable when contrasted with wired network.
- Scalable—suits the expansion of more nodes.
- Improved Flexiblibility.
- Robust because of decentralize organization.
- The network can be set up at wherever and time [1].

Disadvantages of MANETs

- Limited resources and physical security.
- Intrinsic shared trust defense less against attacks
- Lack of authorization offices.
- Volatile network topology makes it difficult to recognize malicious nodes.
- Security protocols for wired networks can't work for ad hoc networks [2].

MANET Architecture

The nodes in a MANET can be characterized by their capacities. A Client or Small Mobile Host (SMH) is a node with decreased handling, stockpiling, correspondence, and power resources. A Server or Large Mobile Host (LMH) is a node having a bigger share of assets. Servers, because of their bigger limit contain the entire DBMS and bear essential obligation regarding information communicate and fulfilling customer inquiries. Customers normally have adequate assets to reserve segments of the database and putting away some DBMS question and preparing modules [4]. As both customers and servers are mobile, the speed at which the network topology changes can be quick. Assortments of systems have been proposed to aid the routing assignments of MANET. New protocols were essential as the protocols for settled foundations and static networks don't perform well when node mobility is incorporated [5].

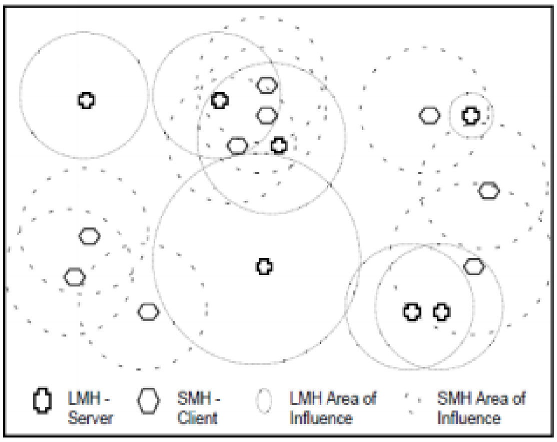

Figure 2 : Nodes of a MANET

Network nodes may work in any of three modes that are intended to encourage the lessening in power utilized: Transmit Mode: this is the mode utilizing the most power.

Characteristics

Wirelesses MANET do not have an underlying fixed infrastructure. Some of the salient features of such networks are summarized below:

- An ad hoc network can be created or deployed at the spur of the moment.
- Mobile hosts can “join” in and move out of the network at any time.
- Mobile nodes within one another’s radio range can communicate directly via radio links whereas nodes not in direct range use other mobile nodes as relays.
- The network topology is continually changing thus of nodes participate and moving out.
- Owing to the lack of an underlying infrastructure with dedicated routers and gateways, the individual mobile nodes carry out the packet forwarding, routing and other network operations themselves.
- Nodes are battery and bandwidth constrained, which makes energy saving a critical issue.

Intrusion Detection systems

An IDS is a device that observers network exercises for strategy infringement and produces reports to an administration station. There are diverse Types of IDS Active and passive IDS

- Network Based and Host Based IDS
- Knowledge Based and behavior Based IDS

IDS in MANETs

Intrusion is any arrangement of activities that endeavor to involve the respectability, secrecy or accessibility There are three main modules of IDS are Monitoring, Analyses, Response. The Monitoring Module is responsible for controlling the collection of data. Analyses Module is responsible for deciding if the collected data indicated as an intrusion or not. Response Module is in charge of oversee and utilizing the reaction activities to the interruption. Because of the constraints of most MANET routing protocols, nodes in MANETs expect that different nodes dependably participate with each other to relay data.

This supposition leaves the attackers with the chances to accomplish huge effect on the network with only maybe a couple compromised nodes. To beat this issue, intrusion-detection system (IDS) ought to be added to upgrade the security level of MANETs. On the off chance that MANET knows how to the distinguish the assailants when they enters in the system, we will ready to totally evacuate the potential harms brought about by traded off hubs at the first run through. IDS generally go about as the second layers in MANETs. Furthermore, it is an awesome supplement to leaving proactive methodologies. So IDS is vital part of protecting the digital foundation from attackers [11].

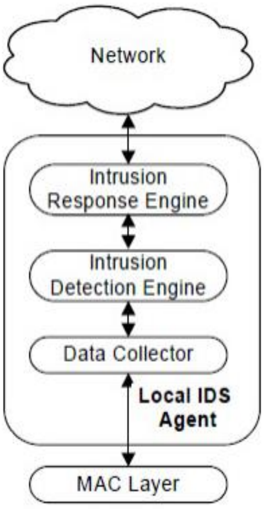

Figure 3 : Intrusion detection System

Background of intrusion detection system (IDS)

An IDS can be characterized as the instruments, strategies, and assets to help recognize, evaluate, and report unapproved or unapproved network movement. Intrusion detection is normally a piece of a general security framework that is introduced around a framework or gadget and it is not a remain solitary assurance measure [12]. The reason for intrusion detection is to fill in as an alert instrument for a computer system or a network. It gives data of undesirable or acting mischievously components and disengages those components to deny them from the PC or network resources. It is possible to identify three main modules in an IDS: a Monitoring Module, controlling the collection of data, an Analysis Module deciding if the data collected indicate an intrusion or not, and a Response Module managing the response actions to the intrusion Figure-1. A few suppositions are made all together for intrusion detection systems to work [13]. The First presumption is that client and program activities are observable. The second supposition, which is more critical, is that ordinary and nosy exercises must have particular practices, as interruption location must catch and investigate framework movement to decide whether the framework is under attack. Contingent upon the detection strategies utilized, IDS can be arranged into three fundamental classes [14]:

- Signature or misuse based IDS
- Anomaly based IDS,
- Specification based IDS, which is a hybrid of both the signature and the anomaly based.

In the interim, the anomaly based IDS endeavors to identify exercises that contrast from the typical expected framework conduct. This recognition has a few methods, i.e., insights [19], neural systems [20], and different procedures, for example, immunology [21], data mining ([22], [23]), and Chi-square test usage [24]. Also, a great scientific categorization of wired IDS was displayed by Debar [25]. The particular based IDS monitors' present conduct of frameworks as per details that portray craved usefulness for security- critical entities. A mismatch between current behavior and the specifications will be reported as an attack. Anomaly detection [Figure-2] constructs its thought in light of measurable conduct demonstrating and anomaly detectors search for conduct that strays from typical framework utilize. The audit data is changed to an arrangement factually practically identical to the profile of a client. The user's profile is created powerfully by the framework (for the most part utilizing a gauge manage laid by the framework executive) at first and in this manner refreshed in light of the client's utilization. Edges are regularly dependably related to every one of the profiles. On the off chance that any examination between the review data and the user's profile brought about deviation crossing an edge set, an alarm of intrusion is declared. This sort of detection systems is appropriate to recognize obscure or beforehand not encountered attacks.

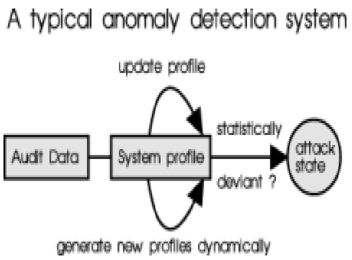

Figure 4: Examples of anomaly detection system

The second kind of model constructs its location in light of an examination of parameters of the user's session and the user's orders to a lead base of strategies utilized by attackers to infiltrate a framework. Known attack strategies are what this model searches for in a user's conduct. Since this model looks for patterns known to cause security problems, it is called a "misuse" detection model [Figure-3].

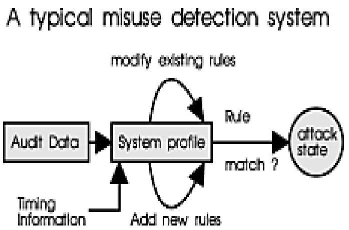

Figure 5 : Examples of a misuse detection system

It is obvious that the enemies, knowing that intrusion prevention and detection systems are in our networks, will attempt to develop and launch new types of attacks. In anticipation of these trends, IDS researchers are designing techniques for combining anomaly and misuse detection, and system architecture for distributed and coordinated intrusions.

Trust Model

We characterize trust [26] as a firm confidence in the ability of a substance to go about not surprisingly to such an extent that the conviction is not a settled esteem related with the element, rather it is subject to the behavior of the entity and applies only to the given context within a defined time. It is apparent from the definition that any trust model performs the following – to make decisions depending on the trustworthiness of nodes, and to collect and maintain the evidence to evaluate the dependability of nodes.

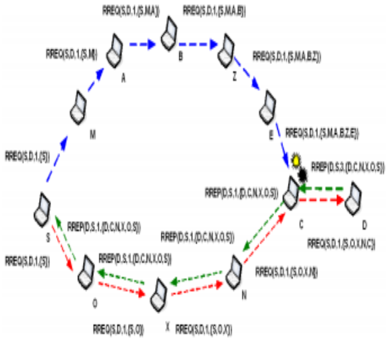

Figure 6 : Route Discovery Cycle for DSR protocol

Our trust demonstrate helps the DSR protocol in settling on choices for the accompanying cases – to acknowledge or dismiss a newfound route from a route disclosure cycle, to record or dispose of a course from a sent packet, to pick a route from accessible courses for a destination, to choose whether to send a packet to a next- hop,or to forward a packet on behalf of a previous-hop. The decision for each of the cases is dependent on the corresponding trust evaluation. In turn, trust evaluations are based on both the direct and recommended trust held for one or more nodes depending on the evaluated case.

III. Problem Formulation

In this research we investigate the intrusion detection that is based on trust, network etc. IDS on MANETs use a variety of IDS approach. The most usually proposed IDS approach to date is specification-based detection. This can detect attacks against routing protocols with a low rate of false positives. However, it cannot detect some kind of attacks, such as DoS attacks.

IV. Proposed Methodology

In our proposed work,trust is calculated by sending the Route Request (RREQ) packets to the network then the target node send Route Reply (RREP) packet. Now we calculate RTT (Round Trip Time) for calculating the distance between the sender and destination nodes. We select the path by taking the shortest RTT and then form clusters. Calculate the energy of every node in cluster and select cluster head of maximum energy. Cluster head forward the data from source to destination. This method removes the chance of malicious node from the network.

Proposed algorithm

```
Step:1   Initialize network
Step:2   If sender has data
Then it sends RREQ to the neighbour nodes
Else
Exit
Step:3   Packet reached to destination through all
         routes
Step:4   Now target node send RREP packet to
         sender
Step:5   Calculate RTT for distance between sender
         and receiver
         RTT = Outgoing trip time + Incoming trip
         time
Step:6   Cluster formation performed
Step:7   If (Energy of node = max)
Node is cluster head
Else
Cluster member
Step:8   Forward data from cluster heads towards
         destination
Step:9   Data reached to the destination from trusted
         nodes
Step:10  Exit
```

Simulation Setup and Results

We simulate a network of sensors in a 250m×250m sensing field. There are hundred sensor nodes (n = 100) are randomly distributed in the field. For doing this the horizontal and vertical coordinates on every sensor are randomly taken between 0 and 100. The sink is taken at the corner, so the multipath fading error is considered in the system. Maximum distance from sink to any node will be approximately equal to p2Ax which is greater than D0 = 87m. We set the initial energy of the normal sensor node to EI = 0:5 joules. The values set is just the simulation any value can assign to it.NS2 simulator is used for the implementation of proposed work. Network Animator and graph are the output generated which show the performance of the work.

NAM: Nam is a Tcl/TK depend animation tool for performing simulation of network traces and valid packet traces of world. It helps to packet level animation, topology layout, and different data inspection tools.

Trace file: The file written by an application (or by the Coverage Server) to store up coverage information or on the whole network information and In NS2, it is called as Trace File. Trace files log each packet, every occurrence which arose in the simulation and are utilized for study.

Xgraph The xgraph program draws a graph on an X show given data examine from either info files or from standard i/p if no files are indicated. Xgraph in ns2 is used to plot the network parameter distinctiveness like throughput, delay, jitter, latency etc.

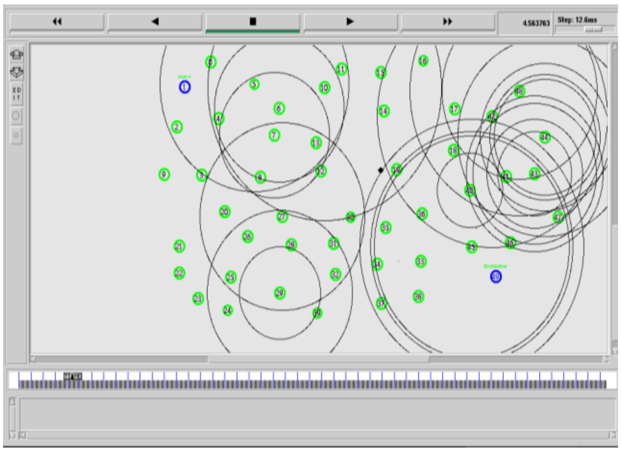

Figure 7: Communication Start

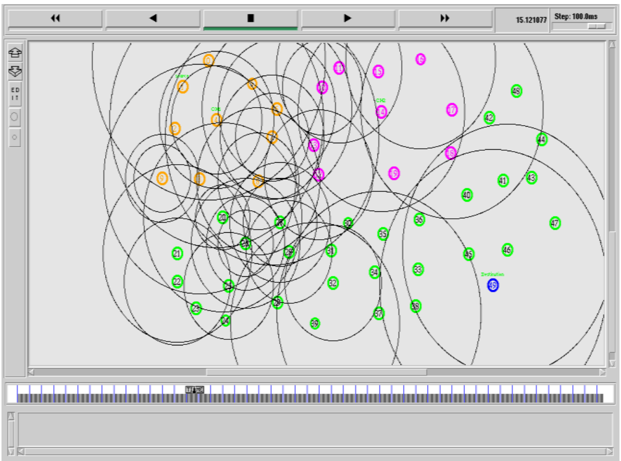

Figure 8: Nodes communicate after forming clusters

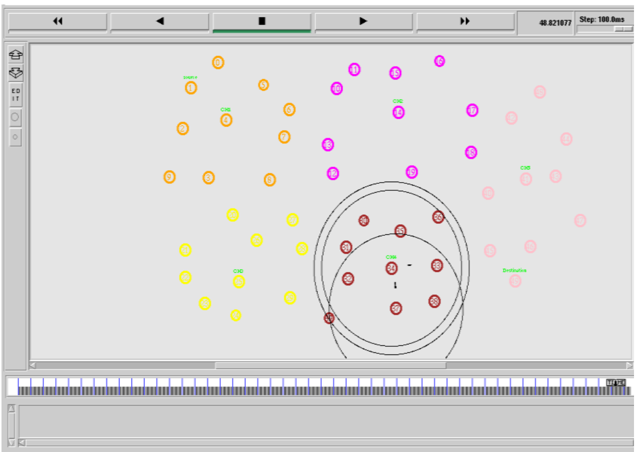

Figure 9: Communicate till data reached to destination

Xgraph: Results in graphical form: 1. Packet Delivery Ratio: It defines as the fraction of packets deliver from source in the direction of destination. The graph represents a PDR graph among base approach as well as proposed approach. This PDR value is enhanced in proposed than an existing approach.

Packet Delivery Ratio = No. of packet received / No. of packets sent

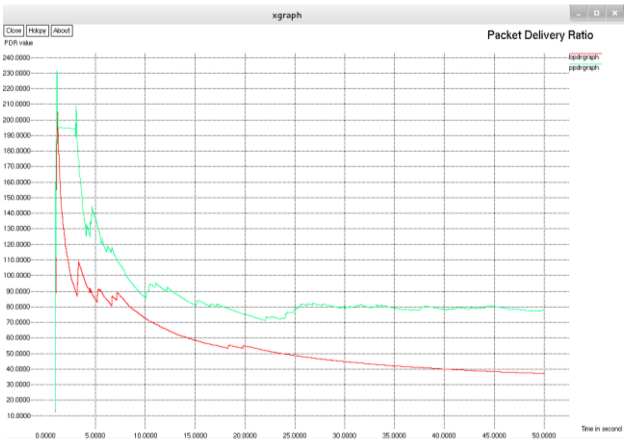

Figure 10 : PDR Graph

1. Throughput: The transmitting of data lying on bandwidth is call as throughput. The graph signifies a throughput graph among base approach with proposed approach. The throughput of the proposed approach is fine than the presented approach.

Throughput (kbps) = (Receive size/(stop time - start time)*1/60

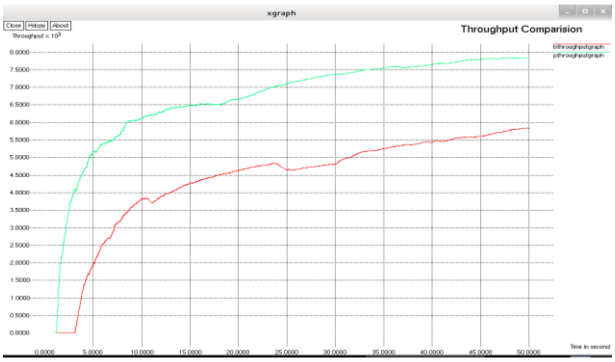

Figure 11 : Throughput Graph

2. Energy: Determine of the ability of a system to change. Initial energy (Transmitting) and Energy loss (Receiving) remaining Residual.

Energy = Initial Energy / Number of node in Route or Remaining Energy

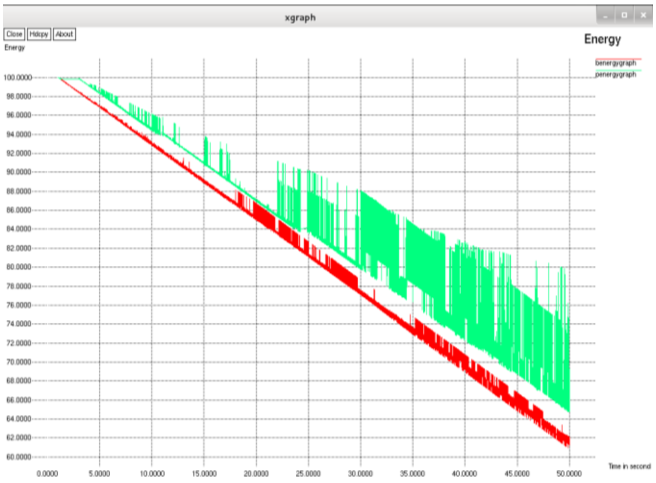

Figure 12 : Energy Graph

3. Routing overhead: It is defined as the flooding of information in the n/w transmitted by application, which utilize a bit of easy to get to transfer rate of communication protocols. The graph represents a routing overhead graph among base approach as well as proposed approach. The proposed approach has an extra overhead than the base approach. Since the overhead be supposed to be minimum except as the routing enhances in the proposed work the overhead also increases.

Routing overhead = No. of packets control in particular time.

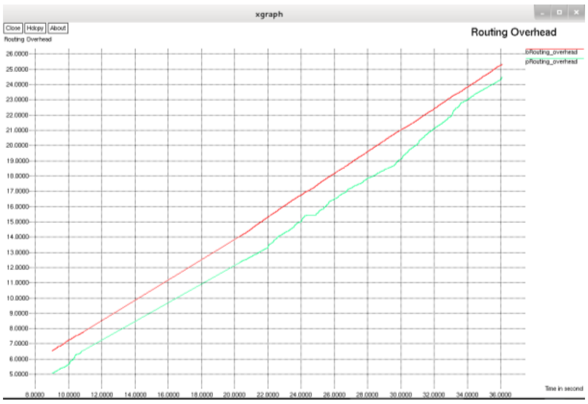

Figure 13 : Routing overhead Graph

V. CONCLUSION

A MANET is a gathering of wirelessly mobility nodes forming a transitory network deprived of any established substructure. The nodes are autonomously to move and establish themselves into a network. MANET doesn't necessitate any static substructure e.g. base stations; so, it's a good networking excellent for connecting mobility devices spontaneously and rapidly. Trust is normally accomplished thru indirect trust mechanisms with agencies servers and trusted certification authentication in wired networks. However, to establishing the indirect trust mechanism necessitates certain mechanism for start authentication and is usually behave with physical or locality-depend authentication schemes. Trust founding in MANET is still uncover and challenging area. The MANET behavior is depending on trust your neighbor relationships.

VI. REFERENCES

[1]. Aarti, Dr. S. S. Tyagi "Study of MANET: Characteristics, Challenges, Application and Security Attacks" Volume 3, Issue 5, May 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[2]. Md. MahbubulAlam, And TanmoonTazShetu, "A Report submitted to sadiahamidkazi of computer science and engineering department of brac university in fulfillment of the requirements for thesis work" April – 2011.

[3]. AikateriniMitrokotsa, Christos Dimitrakakis, ―Intrusion detection in MANET using classification algorithms: The effects of cost and model selection‖, Ad Hoc Networks, Volume 11, Issue 1, January 2013, Pages 226-237.

[4]. Gruenwald, L., Javed, M., and Gu, M. Energy-Efficient Data Broadcasting in Mobile Ad-Hoc Networks. In Proc. International Database Engineering and Applications Symposium (IDEAS '02), July, 2002.

[5]. Lee, S., Su, W., and Gerla, M., "Wireless Ad Hoc Multicast Routing with Mobility

Prediction," Mobile Networks and Applications, 6(4): pp. 351-360, 2001.

[6]. Liu, J., Zhang, Q., Li, B., Zhu, W., and Zhang, J., "A Unified Framework for Resource Discovery and QoS-Aware Provider Selection in Ad Hoc Networks," ACM Mobile Computing and Communications Review, 6(1): pp. 13-21, 2002.

[7]. Singh, S., Woo, M., and Raghavendra, C. Power Aware Routing in Mobile Ad Hoc Networks. In Proc. 4th International Conf. on Mobile Computing and Networking (MOBICOM '98), pp. 181-190, October, 1998.

[8]. Mrs.Padma .P, Mr.R.Suresh "Literature Survey on latest research issues in MANET" ISSN: 2278 – 1323 International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013.

[9]. KetanNadkarni "An Intrusion Detection Scheme for Wireless Mobile Ad hoc Networks based on DSDV Protocol" August 29, 2003.

[10]. Ms. ApurvaKulkarni, Mr.PrashantRewagad ,Mr.MayurAgrawal "Literature Survey on IDS of MANET" International Journal of scientific research and management (IJSRM) ||Volume||3||Issue||9||Pages|| 3549-3552||2015||.

[11]. Ranjit j. Bhosale, Prof. R.K.Ambekar "A Survey on Intrusion detection System for Mobile Ad-hoc Networks" Ranjit j. Bhosale et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7330-7333.

[12]. A Survey on MANET Intrusion Detection: Satria Mandala satriamandala@hotmail.com Faculty of Science and Technology, Department of Informatics Engineering, State Islamic University of Malang Jl. Gajayana 50 Malang, Indonesia, Md. AsriNgadi dr.asri@utm.my Faculty of Computer Science and Information System, Department of Computer System and Communication, UniversitiTeknologi Malaysia (UTM) Skudai - Johor, 81310, Malaysia.

[13]. Y. Zhang, W. Lee and Y. Huang. 2003. Intrusion Detection Techniques for Mobile Wireless Networks. ACM/Kluwer Wireless Networks Journal (ACM WINET). 9(5).

[14]. A. Hijazi and N. Nasser. 2005. Using Mobile Agents for Intrusion Detection in Wireless Ad Hoc Networks. In Wireless and Optical Communications Networks (WOCN).

[15]. T. F. Lunt and R. Jagannathan, et al. 1988. IDES: The Enhanced Prototype C a Realtime Intrusion- Detection Expert System. Technical Report SRI-CSL-88-12, SRI International, Menlo Park, CA.

[16]. M. Esposito and C. Mazzariello, et al. 2005. Evaluating Pattern Recognition Techniques in Intrusion Detection Systems. The 7th International Workshop on Pattern Recognition in Information Systems. pp. 144-153.

[17]. S. Kumar and E. Spafford. 1994. A Pattern Matching Model for Misuse Intrusion Detection. The 17th National Computer Security Conference. pp. 11-21.

[18]. P.A. Porras and R. Kemmerer. 1992. Penetration State Transition Analysis C a Rule-Based Intrusion Detection Approach. The 8th Annual Computer Security Application Conference. pp. 220-229.

[19]. W. Lee, S.J. Stolfo and K.W. Mok. 1999. A Data Mining Framework for Building Intrusion Detection Models. IEEE Symposium on Security and Privacy. Oakland, California.

[20]. G. Florez, S.M. Bridges and R.B. Vaughn. 2002. An Improved Algorithm for Fuzzy Data Mining for Intrusion Detection. The North American Fuzzy Information Processing Society Conference, New Orleans, LA.

[21]. N. Ye and X. Li, et al. 2001. Probabilistic Techniques for Intrusion Detection Based on

Computer Audit Data. IEEE Transactions on Systems, Man, and Cybernetics. pp. 266-274.

[22]. H. Debar, M. Dacier and A. Wespi. 2000. A Revised Taxonomy for Intrusion-Detection Systems. Annales des Telecommunications. pp. 361-378.

[23]. C. Ko, J. Rowe, P. Brutch and K. Levitt. 2001. System Health and Intrusion Monitoring Using a hierarchy of Constraints. In: Proceedings of 4th International Symposium, RAID.

[24]. Intrusion Detection in Wireless Ad-Hoc Networks: FoongHengWai hengwai.foong@nus.edu.sg> Yin Nwe Aye Ng Hian James nghianja@comp.nus.edu.sg: CS4274 INTRODUCTION TO MOBILE COMPUTING.

[25]. Sundaram A. An introduction to Intrusion detection, http://www.acm.org/crossroads/xrds2-4/intrus.html.

[26]. S. Yan Lindsay, Y. Wei, H. Zhu and K. J. R. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks". IEEE Journal on Selected Areas in Communications, Vol-24(2), pp. 305-317, 2006

[27]. W. J. Adams, N. J. Davis, "Toward a Decentralized Trust-based Access Control System for Dynamic Collaboration," Proc. 6th Annual IEEE SMC Information Assurance Workshop (IAW'05), 15-17 June, 2005, West Point, NY, pp. 317-324.

[28]. R. Mayer, J. Davis, and D. Schoorman, "An Integrative Model of Organizational Trust," The Academy of Management Review, vol. 20, pp. 709-734, 1995.

[29]. A. Jøsang, "The right type of trust for distributed systems," Proceedings of the 1996 workshop on New security paradigms, 1996.

[30]. D. E. Denning, "A new paradigm for trusted systems," Proceedings on the 1992-1993 workshop on New security, 1993.

[31]. Vishnu Balan E, Priyan M K, Gokulnath C, Prof.Usha Devi G , "Fuzzy Based Intrusion Detection Systems in MANET ", Elsevier 2015.

[32]. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc.2010.

[33]. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based pproach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile May 2007

[34]. A. Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET," in Communications in Computer and Information Science, vol. 147. New York: Springer-Verlag, 2011.

[35]. B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[36]. N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE 2007.

[37]. J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE 2004.

[38]. T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer-Verlag, 2008.

[39]. Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in P+roc. 4th IEEEWorkshop Mobile Comput. Syst. Appl., 2002.

[40]. Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom,Atlanta, GA, 2002.

[41]. G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routin