Journal of Engineering Sciences

Vol 11, Issue 7,July/2020

ISSN NO:0377-9254

Enhanced Secure communication AODV routing protocol using SVM in MANETS

MAJETI JYOTHI PRIYA
M.Tech Research Scholar
Department of CSE
UshaRama Engineering college of engineering and technology
jyothipriyamajety@gmail.com

Dr. SUBRAMANI ROYCHOUDRI
Professor & Head of the Department
Computer science and engineering
UshaRama Engineering college of engineering and technology
csehod@usharama.in

Abstract:

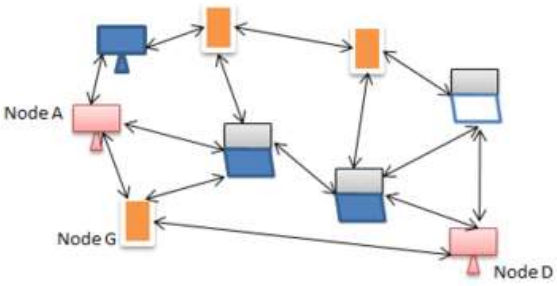
MANET topology is more complex due to this functionality, which is more complicated and anxious within this network building mechanism and hence nodes are more prone to compromising and are primarily vulnerable to Denial Service Assail (DoS) assailing by malicious nodes or intruders[6]. Attackers have used this idea to conduct DoS attacks similar to floods; the branded attack on MANET is a black hole and gray hole. In this post, we have projected a new automated protection system that uses SVM in defense of malicious AODV attacks. The method proposed uses machines to classify nodes as malevolent. In MANET 's context, such as malicious nodes which over time change misconceptions or rapid changes in environmental factors such as movement speed and communication range are considerably resilient to these changes. This paper presented an algorithm used to track MANET behavior by a specific node to detect attacks on ad hoc networks based on secure data transmission. Compared to conventional models, the new model reveals that it has improved results in terms of detection of malicious users and also an increased package delivery volume.

Keywords: MANET's, Denial Service Attack (DoS), security, SVM

1. Introduction:

A modern wireless networking model for handheld nodes is ad hoc networks. The growing development of wireless apps has rendered mobile ad hoc networking (MANET) [5] an exciting and significant technology in recent years. It is a difficult job to supply MANET with sufficient protection controls. Originally, it is simple and complicated to handle wireless communications. In fact, wireless messages are conveniently passively added or changed. This ensures the insecure wireless networks will be compromised by a broad variety of methods like the infiltration of routers, the intrusion of messages and lack of secrecy. It helps enemies to catch and assault them violently. Proper (tamper resistance) safeguards are required to deter attackers from stealing sensitive knowledge. Also with these measures, we can not rule out the risk of sacrificing a portion of the nodes. It makes for threats from the network. Third, the lack of supporting infrastructure and complex topologies renders most of the current cryptographic algorithms useless because they have not been built for this dynamic setting. Some static protection system [19] [20] will not be enough. Mechanisms for protection

Figure 1: Ad-hoc Network



A Safe Routing Algorithm can respond to these improvements in topology on-the-fly for MANET [21]. Fourthly, a small power tool (packaging, solar panel etc.) can be present in several wireless nodes. For ad-hoc sensor networks that is particularly true. A limited energy allocation will take security solutions into consideration. Eventually, there are thousands of nodes in an ad hoc network. To control such a wide network, protection frameworks should be scalable. Our MANET algorithm is based on the widely accepted methodology of route discovery

based on transmitted demand packets. Most precisely, the relaying intermediate nodes apply their identificator (e.g. IP address) on the query packet header as query packets enter the network. When one or more requests reach the destination, answers containing the accumulated routes will be returned to the querying node; one or more of these routes can be used by the source to pass on its data. Our suggested Secure Routing Protocol (SRP) can be used as an extension of a variety of current routing algorithms by utilizing this simple path query communication method. Included in this are two algorithms which can be inherently generalized in order to include SRP: The Dynamic Source Routing (DSR) [1] and the Zone Routing Protocol [2] IERP [3] system. In addition, other protocols such as ABR[4] could be paired with SRP and minor modifications to meet the SRP security objectives.

Basically , there are two methodologies that can give security in MANETs in particular: counteractive measures and methodologies based on identification[7,8,9,10]. MANETs [11,12,13,14] thoroughly find prevention-base methodologies. The difficulty with these counteractive measures is that a central administration framework is required, which in distributed schemes, such as MANETs, may not be sensible. As a consequence, discovery-based approaches are well-suited to identify dangerous tasks, such as pitch, gapless, sybil assaults, packs, and sleep attacks, etc. Many current confidence related recognition strategies do not use direct data and secondary data (acquired from external) hubs in the interim to approximate the stock of the center. Specific data is called "backhanded awareness," to combine experience, and second hand data obtained from outside. The unreliable [15,16,17] confidence respect evaluation is conducted in many second-hand methodologies. Thus a hybrid trust management storyline, which allows use of late development in undefined reasoning, is introduced.

2. Literature work:

An algorithm for efficient routing in MANET has been developed based on Friend-dependent Ad Hoc routing with challenges for ensuring protection (FACES). The connection was developed in this algorithm by the sending of the task and the trustworthy node lists to the source node. Depending on the volume of data they have shared and the relationship with other nodes, they chose the friend node list. This allowed the network the malicious nodes which could not participate in the transmission successfully to be detached. The main advantage is that traffic can not be taken care of in the nodes while the packets are passed to their neighbours. Information was obtained successfully about the hostile nodes. (Chapel Sanjay et al. 2011)

A leading collection focused on selfish nodes was established in order to optimize the usage of resources across all the nodes and increase the life cycle of a MANET. The members have been elected nodes with the remaining capital. For achieving the target, two main obstacles have been established. First, nodes are greedy and lie about remaining power to avoid data transmission from being chosen. Furthermore, total cost management. The approach was sought based on the system architecture principle to prevent the issue of selfish nodes. This encourages the nodes to engage freely in the application process as reputations. The bonus number is focused on the Vickrey Clarke and Groves (VCG) model to insure that every node is honest. A set of local selection algorithms were implemented at low costs for the optimal selection problem. (Noman and others 2011).

Authentication is a significant method for protecting against MANETs who are extremely safe for protection. The recognition of malicious events was also critical for intrusion detection systems (IDSs) in MANETs. All of these methods have been used to satisfy the MANET protection and resource criteria. This method was used in part by the decision-making mechanism Measurable Markov (POMDP). This method can be used to address the issue with a node modification in a large network. (Shengrong et coll. 2013). 2011.

In MANETs, cognitive radios (CRs), which are designed to sense the ambient conditions and to change the hidden parameters. CR-MANET data detection (BDDF) attacks, which are designed to give intruders incorrect local range-sensing results which lead to mistaken CR spectrum-sensing choices. A modern, biologically based, cooperative spectrum sensing framework was developed in CR-MANET to combat stationary stable data forgery (SSDF) attacks. The system is focused on the premise that animal groups such as birds, cats, aunts, honeybees and others work out themselves. The machine has the capacity to self-configure and sustain itself. Authentication schemes are used to improve security and efficiency using identity (ID)

based encryption with threshold secret sharing. (Tang et al. 2013). 2012.

In order to limit abuse of privacy across two methods, the trust-enhanced anonymic on-demand routing protocol (Teap) was introduced. Through the original procedure, if the consumer is not given two alerts, he / she would be revealed to all apps as a misbehaving person. When a user wants to send several packets for the same reason to a single device, it is often recognized as a misbehaving device during the second phase. The TEAP protocol was built on the basis of knowledge transmitted. This is a principle of cryptography used in the hidden identification of misbehaving network subscribers. (Kandhasamy and Muthumanickam 2013).

A lot of research was performed in the development of an adaptable routing protocol for MANET to connect intelligent (SI) swarm procedures. The mobile nodes (MNs) found in current MANETs can monitor the network location and the processing of data. The MANET will also be made conscious of context by means of the contextual management expertise of MNs. MANETs were proposed with a modern versatile, bio-inspired routing protocol. The suggested convention has two objectives (1) To consider a consistent direction based on secure nodes in terms of its stability, with the aid of a local tracking capacity (2) to promote calculation distortions utilizing pheromone smoothing. (Kiran and Ram 2013). 2013.

To give a high degree of protection, an Effective Routing (ALERT) approach focused on Anonymous Platform was suggested. ALERT divides the system field into zones and randomly selects the routing path nodes in zones as intermediate relay nodes. In fact, ALERT ensures protection for origins, locations and routes. ALERT is providing greater public protection and reduced costs than other privacy routing approaches while analyzing the tests. (Shen and Zhao 2013). Practice. In the latest study into multi-hop wireless networking and cellular networks , data sharing has received considerable interest. Due to the lack of successful constructive routing schemes with high source routing capacities, MANET data transmission was not used. MANET has also established a Light-Wight Proactive Target Routing Agreement (PSR). PSR has far less total heading than the destination-sequenced distance vectour routing protocol to facilitate source routing than distance vector routing. (Columbia and others, 2014).

Thanks to MANETs' complex topology, nodes are able to switch. To improve security, the rekeying process is necessary to secure a communication method for the Multicast Transmission Cluster. The cluster connectivity is achieved through the allocation by the centralized key manager of private key portions of the nodes. The correspondence between clusters is carried out by gathering data with private key shares. When a node is connected to the cluster, the rekeying procedure is used. Recovery technology has small overheads, lowered operating costs and improved performance. (Duraisamy and Vennila 2014).

A new theoretical framework has been established with recent developments in field theory and it serves as a valuable weapon for countering threats, as well as securing network infrastructure. The theory of the game can give you a useful suggestion in MANETs to focus on the security issue. Throughout the protection game system, it considers primarily two players: an attackers and a guard. It is specific to a distributed network rather than to uncentralized networks like MANET. Each node is treated autonomously in this model. A novel theoretical entertainment strategy has been tested with various MANET health matches. The mean field fun hypothesis offers the question of a large number of players an important numerical tool. (Israel and other 2014).

MANET has a range of unplanned portable devices, such as complex topology and free remote media, which may contribute to other security weaknesses. For that purpose, a trust administration protocol was proposed that improves safety in MANETs. The confidence show has two sections in the proposed trust management plot: the direct observer 's trust and the indirect observer 's trust. Both observers gained information, the Bayesian inference and DST made confidence estimates. In a node the trust values have been stored and this knowledge routing has been used. This was able to distinguish packets and packets and lost the other packets as wireless contact became poor. The distribution level is strong and the end-to - end period has improved. Zhexiong et al . 2014, respectively.

It is interesting that machine code has a nice property of proper protection, which can be effectively encrypted. To order to do this, P-Coding introduced

a lightweight encryption strategy for protection to an energy intensive way to organize encoded MANETs. The key aim of P-Coding, before carrying out device coding operations, is to encourage the source to arbitrarily permit images in any item. Detectives can not find coding vectors for correct decoding, and therefore no important information can be obtained without knowing the modification. P-Coding offers protection relative to other encryption schemes because of its light weight nature (Zhang et al . 2014).

For node communication, MANETs make nodes work with one another an essential requirement. This need will cause legitimate safety issues in the view of hostile nodes, these nodes, for instance, may disrupt the guiding process. Throughout this particular situation it is a struggle to combat or identify hostile nodes, gray or black hole threats. This topic has been explored by the preparation of the DSR-based management framework known as the CBDS, which combines the advantages of constructive and reactive safeguarding principles. To order to accomplish the specified goal, the CBDS approach used a reverse tracing methodology. (Jiang- Ming and coll. 2015).

Nodes may be modified in nature in MANETs. In MANETs that have their difficulty in numerous safety attacks and defective operating safely while securing their properties and conducting secure routing of nudity, coordination between adaptable nodes is more essential. Game theory is a tool from now on that discusses strategies and acknowledges egoism. This is used in applications to distinguish the harmful behavior. A remarkable answer to signage games for clarifying incomplete information by combining procedures and payments to players who constitute balance. Perfect Bayesian equilibrium (PBE) gives Methods of PBE

For serious scenarios like military , law enforcement and emergency rescue and recovery, MANET's are both useful and compatible. MANETs need communication protection and privacy, particularly for primary routing protocols, while working in hostile or suspicuous settings. Contrasting with the bulk of networks, where correspondence is focused on long lasting identities (addresses), it has been proposed to use the data protection-friendly routing scheme in suspicionable MANETs (PRISM protocol).

A source of data can not reach the destination on broad networks in a single hop, requiring traffic via multiple hops. This is why a spatial and self-organizing coordinate routing approach was built by early-inondation and hierarchical protocols utilizing the last decade. The above has already implemented by the IETF Low Powers and Loss Networks (ROLL) workgroup, through the Internet Technology Task Force, through the MANET Laboratory. The latter is now moving towards standardization. For the sequential structure of the protocol, the template for routing in WSNs and separate previous thresholds is used. In contrast with other protocols the implementation of IETF ROLL was more stable and effective. (Switzerland et al . 2011).

Avoiding the incompatibility of centralized MANET-based hash table routing between a physical network (PT) and a functional identity system of MANETs will eliminate the problems of longer paths, large track-straight ratios and increased overhead traffic. A 3dimensional (3D) logical identifier (LS) space (LS) was proposed to address this problem, where every node calculates a successive logical identification (LID) to route packets. The framework also uses the 3D logical identity scheme (3DLIS) to establish single paths by multi-hop manipulation at a node to the destination node (Abid et al. 2013).

That node consists of a route cache, where routes to various destinations are indexed in sequence, in MANET Routing Protocols such as DSR. During the meanwhile, the path cache is able to store several routes such that its accuracy and durability are regularly checked. A way to link consistency cache replacement to MANET has been suggested. The source uses this approach to reach many paths through multipath routing to the destination. The paths acquired are deposited in the cache of the lane. The cache substitution method estimates the connection quality with the aid of the signal strength (RSS) value received. Link cache eliminates connections with a weak RSS rating. At the same time, the time stamp value of each node retains a path cache table periodically. Simulation tests determine the reliability of the cache replacement process. The approach efficiently preserves the path cache and improves device efficiency (Jagadeesan et al . 2013).

Local connectivity for routes establishment and maintenance was extremely important in MANET.

Periodic Hello notifications is a commonly used method for local connections. Unnecessary texting Hello, though, will kill batteries even though mobile devices are not in operation. To erase Hello messages without the bridged detectability of damaged ties (Han et al. 2013), an innovative Hello messaging program was introduced.

The current best practices have been studied in the evaluation of protocols for a multi-hop ad hoc wireless network (MANET). We expand the configurations and parameters used in MANET simulations to incorporate a prior characterisation. You notice that several design falls still occur, which hurt the credibility of the results in effect. In the name of its basic dimensions and parameters, they define the simulation known as "design space." Moreover, the simulation accuracy was improved by utilizing many auxiliary parameters. (Spain et al. 2012).

A routing model was developed that is capable of perceiving MANET mobility states and autonomous routing (Zehua et al. 2014). In this example, nodes count their mobility predictor to see if the network is fairly static or mobile, thus changing the routing parameter to either the estimated number of transmissions (ETX) or the mobility factor (MF). The predicted model takes into account ETX and MF metrics and increases MANET 's total routing efficiency in various usability states. (The Book is also accessible on the Internet).

Recently, owing to the low expense, versatility and usability of mobile apps, MANETs have seen accelerated growth. During the direct wake of a natural catastrophe in which networking infrastructures can be no longer functional or usable, such tools should utilize a secure network. As the connections in such a network will shift easily in the absence of unified control at any moment, routing is seen as the most challenging job. Additionally, certain protocols for routing such as Neighbor

Probabilistic scope rebroadcast (NCPR) is fully secure in the preset variables needed by scenario-based device administrators. However, many certain navigation methods, such as the AODV, utilize the RREQ flooding method to identify a particular path discovery target. While the flood network has improved control, it familiarizes with unnecessary overhead routing leading to deterioration of the scheme 's efficiency. A new routing protocol, Dynamic Connectivity Factor Routing Protocol (DCFP), which is able to prove the status of the simple network dynamically without interferring with a specific connectivity parameter, thus utilizing a novel connectivity factor to decrease the overhead RREQ was proposed. The proposed DCFP tackles the need for predefined NCPR variables. It provides NCPR in terms of electricity usage and the completion of the delay. (Annalysis and Study 2016).

3. Proposed work:

The ad hoc mobile network has attracted growing interest from business, and is a modern form of wireless communication. Mobile ad-hoc networks have to deal with various security risks as in general networking conditions. The routing of the mobile ad hoc network is a critical consideration for network success, considering the complexity of complex network topology. It is obvious that most security threats focus on routing protocols – the weakest part of the ad-hoc mobile network. Within this area there are many experiments and work aimed at developing healthier protocols. However, in every situation, there is no complete routing protocol capable of ensuring the operation of a network. A "safe" protocol is usually only good to protect the network against one specific form of attack. Many studies have done so in conjunction with standard routing protocols to test the efficiency of secure routing protocols.

Present research is minimal

Weak efficiency because of tread instability

Low delivery and performance of packages

Far less pause from end to end.

Within this area there are many experiments and work aimed at developing healthier protocols. However, in every situation, there is no complete routing protocol capable of ensuring the operation of a network. A "safe" protocol is usually only good for safeguarding the network against a particular type of attack. Many studies have done so in conjunction with standard routing protocols to test the efficiency of secure routing protocols. One of the goals of this research is to examine the additional costs in different scenarios by adding a security feature to unsafe routing protocols. The extra charge includes delays in the transmission of packets, a low rate of data packets over the total packets sent, etc.

Advantages:

It improves protection

It improves efficiency by increasing the packet supply and output

Reduces the gap from end to end.

Algorithm

Step1:-Exploration of the path);
We get the RREP packet hop count (hc) and delay (del), count=0;
Step 2:-Malicious transmission of watch packet
Whether (hc<=4 Del>100 Del<10)
(i=0; i<4; i++) By.
Uploading / uploading / evil watcher / receiver;
Whether (ACK > =3)
No malevolent node;
Continue the transmission of data;
}
That's it.
The assailant;
Step3 Goto;
}
}
}
Step3:-node I d storage in suspected tracks;
For (i=0 (transmission); i<=hc; i++)
Id[i] = = = = = =)
Get (middle ID node);
Count = account +1;
Step1 Goto;
}
Step4 Goto;
Step4:-comparison of lists that have been suspected using SVM;
()); /We use sorting in order to compare;
No-of-dop (count) duplicates;
Is (no-of-dup > count-2)
Attacker found-IDs of the node;
}

4. Experimental analysis:

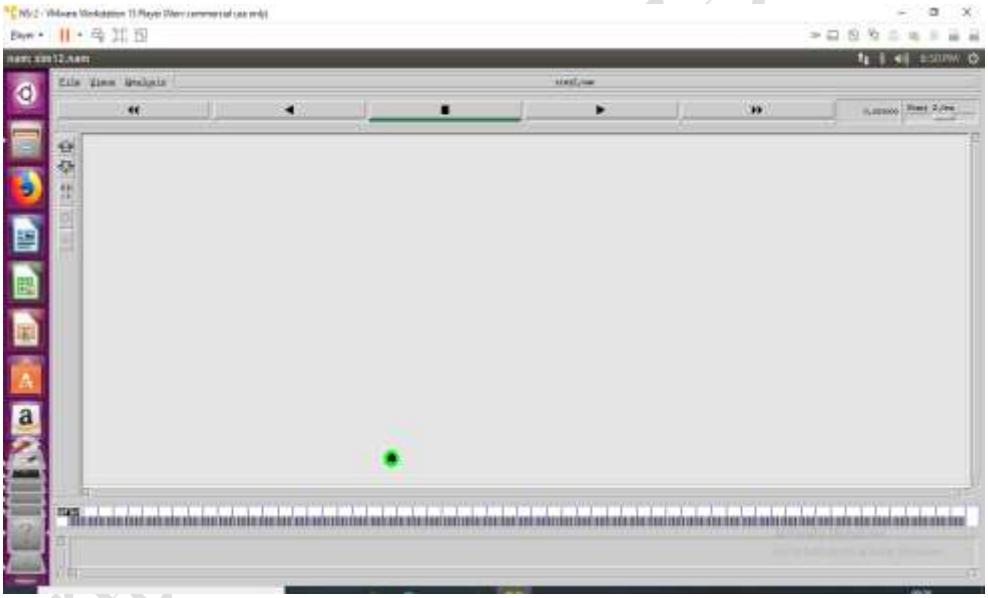


Figure-2 Running of NAM

Here Figure-2 Running of NAM. Network Animator it shows the simulation to the users and the way of nodes are imitated and how the data flow is happened.

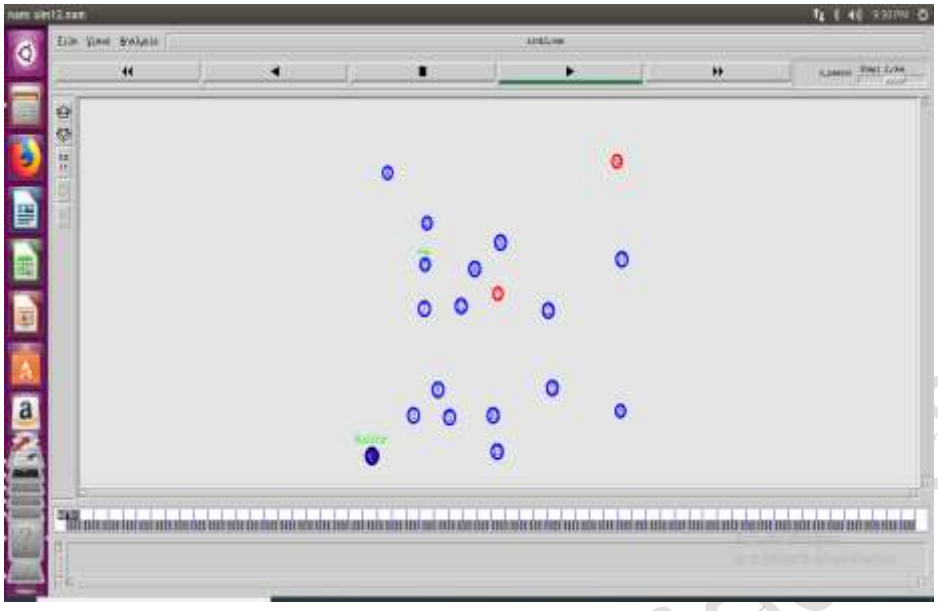


Figure-3 Simulation started

Figure-3 simulation environment and nodes of red colored and blue color. Red color nodes are malicious nodes and blue color nodes are normal nodes.

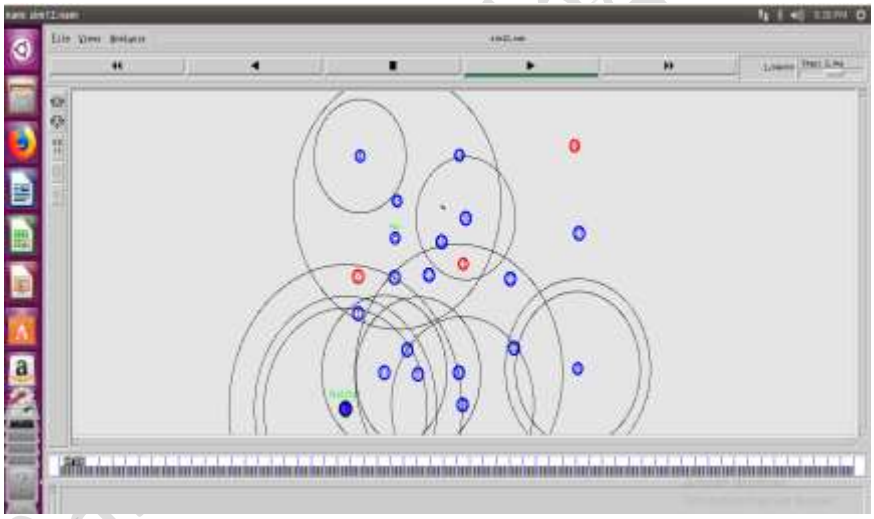


Figure-4 Simulation of secure routing protocol

Fig-5 Comparison for Packet Loss for 50 Nodes in MANEs

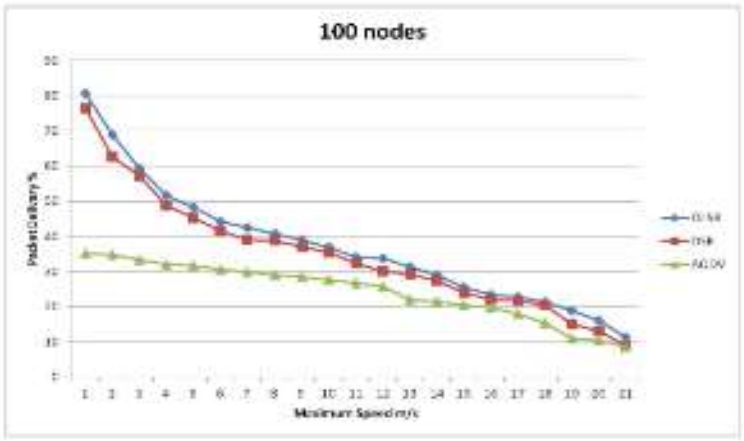


Fig-6 Comparison for Protocols Packet Delivery for 100 Nodes in MANETS

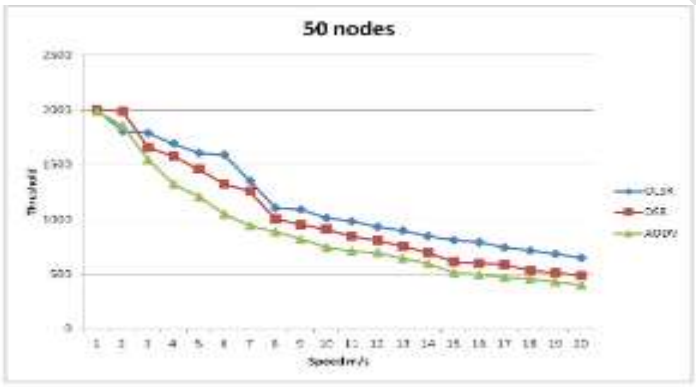


Fig-7: Threshold comparison Protocols for 50 Nodes in MANET

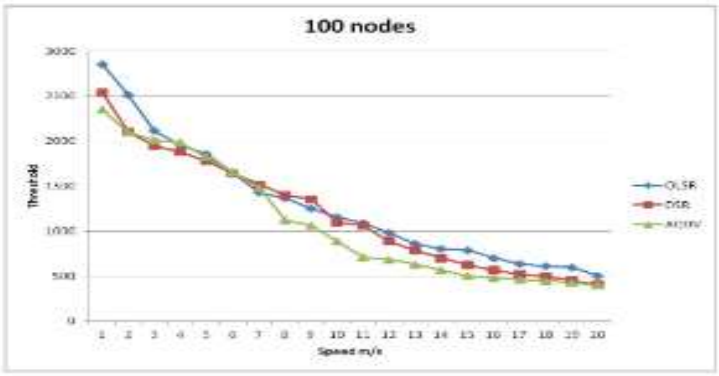


Fig-8: Threshold comparison Protocols for 100 Nodes in MANET

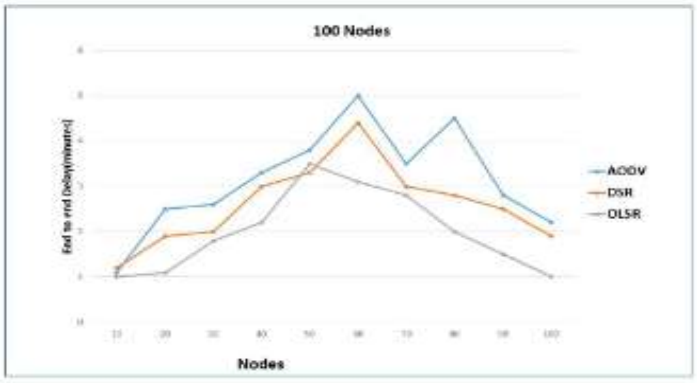


Fig-9 End to end delay comparison Protocols for 100 Nodes in MANET

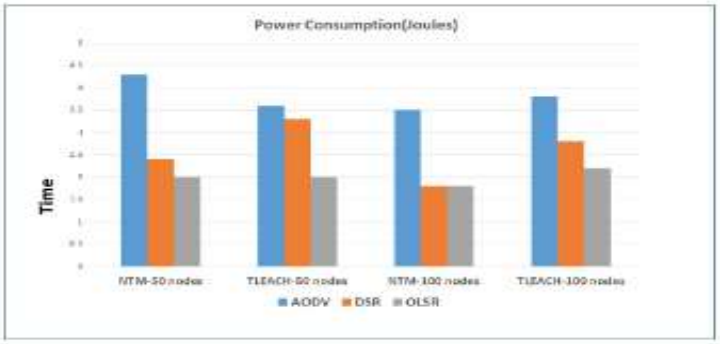


Fig-10: Power consumption comparison Protocols in NTM and TLEACHfor 50 and 100 Nodes in MANET

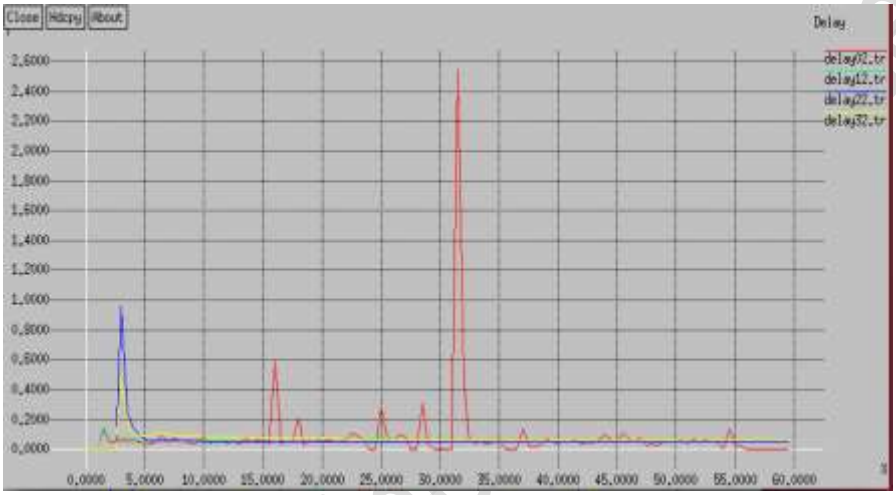


Fig-11: End to end delay comparison Protocols with respect to pause time

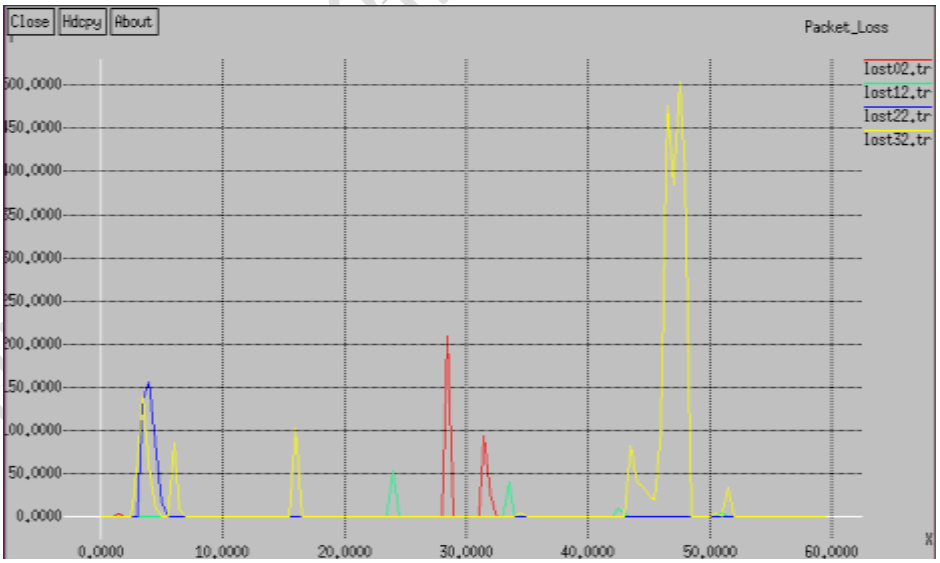


Fig-12: Packet loss comparison Protocols with respect to pause time

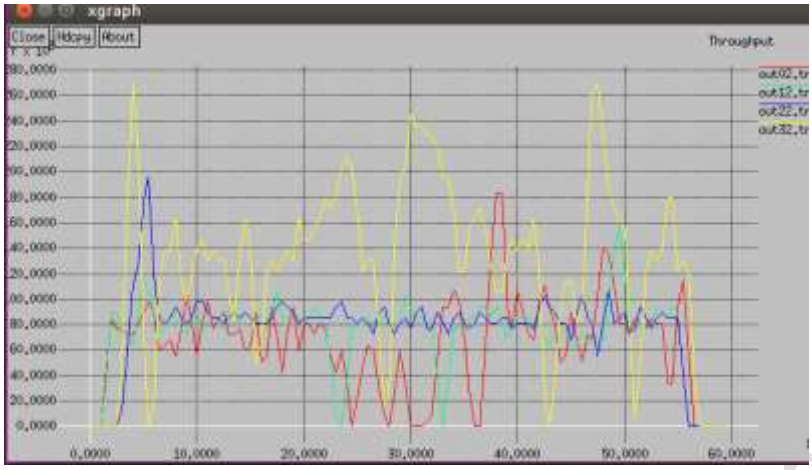


Fig-13: Throughput comparison Protocols with respect to pause time

5. Conclusion

Mobile computing is a new way forward for mobile communication where mobile devices form a self-structured, self-organizing wireless network called a mobile ad hoc network. This is an important part of mobile communication. By addition, mobile ad hoc networks are more susceptible than fixed or hardwired networks to physical security attacks. This paper illustrates various MANETS concepts that can maximize the support of researchers. It 's important to potential computing environments due to its inherent simplicity, lack of resources, quick installation, self-configuration, low-cost applications. The nodes in ad hoc networks are that, verified, more capable and in any shape, particularly when dense deployment, such as battlefield or sensor networks takes place. Altogether, even if ad hoc networks are commonly distributed. Many wireless ad-hoc networks have no network access control and are susceptible to assaults on resource use, where a malicious node injects packets through the network to deplete the capacity of paket-related nodes[76].

To avoid or discourage these attacks, security methods must be used to insure that only allowed nodes may upload data into the network.[77] Such networks, also with authentication, remain susceptible to packet drop or pause attacks that force an intermediate node to drop the packet or postpone the data instead of automatically moving it to the next hop. The suggested prototype suggests an algorithm that detects fraudulent behavior during data transmission in the ad hoc network with precision.

References:

1. C.Perkins, Ad Hoc Networks, Addison-Wesley, 2001.

2. H. Yang, H. Luo, F.Ye, S Lu, and L. Zhang, Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications, 38-47, 2004.

3. Kumar S, Pruthi G, Yadav A and Singla M, Security Protocols in Manet, Second International Conference on Advanced Computing & Communication Technologies, 530-534, 2012, IEEExplore.org.

4. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, Prevention of Cooperative Black Hole Attack in Wireless International Conference on Advances in Human Machine Interaction (HMI - 2016), March 03-05, 2016, R. L. Jalappa Institute of Technology, Doddaballapur, Bangalore, India 978-1-4673-8810-8/16/$31.00 ©2016 IEEE Ad Hoc Networks, North Dakota State University, White paper, 2009.

5. B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, An On-demand Secure Routing Protocol Resilient to Byzantine Failures. Proceedings of the ACM Workshop on Wireless Security, pp. 21-30, 2002.

6. Y. Hu, A. Perrig, and D. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. Proc. of the ACM Workshop on Wireless Security (WiSe), pp. 30-40, 2003.

7. X. Wang, D. Feng, X. Lai, and H. Yu, Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD, Cryptology ePrint Archive, Report 2004/199, http://eprint.iacr.org/, 2004.

8. W. Mehuron, Digital Signature Standard (DSS). U.S. Department of Commerce, National Institute of

Standards and Technology (NIST), Information Technology Laboratory (ITL). FIPS PEB 186, 1994.

9. W. Stallings, "Cryptography and Network Security", Pearson Education, 2007.

10. W. Stallings, Wireless Communication and Networks, Pearson Education, 2002.

11. Perrig, R. Canetti, J. Tygar, and D. Song, The TESLA Broadcast Authentication Protocol. Internet Draft, 2000.

12. C. Kaufman, R. Perlman, and M. Speciner, Network Security Private Communication in a Public World, Prentice Hall PTR, 2002

13. Kimaya Sanzgiri, D.LaFlamme, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth M. Belding- Royer. "Authenticated Routing for Ad hoc Networks." IEEE Journal on Selected Areas in Communications 23.3 (2005): 598-610.

14. Azzedine Boukerche and Yonglin Ren, A Novel Solution based on Mobile Agent for Anonymity in Wireless and Mobile Ad hoc Networks, Q2SWinet'07, Greece, 86-94, ACM, October 2007.

15. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, WIRELESS/MOBILE NETWORK SECURITY, Springer, 2006.

16. Young-Bae Ko, and Nitin H. Vaidya, "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks", MOBICOM'98, 1998.

17. Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang, Resisting Flooding Attacks in Ad Hoc Networks, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05), IEEE Computer Society, 2005.

18. Manel Guerrero Zapata, Secure Ad hoc On-Demand Distance Vector Routing. ACM Mobile Computing and Communications Review (MC2R), Vol 6. No. 3, pp. 106- 107, July 2002.

19. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Communications, vol. 11, pp. 38-47, 2004.

20. S. Sampalli, S. Jamwal, L. Lei, P. Moradiya, S. Parikh, T. Potluri, T. Shingne, A. Thangaraj and A. Trabulsi, "Routing Intrusions on Mobile Ad Hoc etworks: Test bed and Vulnerability Analysis", In Proceeding of Software, Telecommunications and Computer etworks, 2007. SoftCOM 2007. 1-5, ISBN: 978-953-6114-93-1.

21. Kimaya Sanzgiri, Daniel LaFlamme Bridget, Dahill Brian Neil, Levine Clay Shields Elizabeth M. Belding-Royer, Authenticated Routing for Ad hoc Networks, IEEE J. Selected Areas of Communication, vol.23, no.3, pp.598- 610, 2005.

22. S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating Routing Misbhavior in Mobile Ad Hoc Networks. In Proceedings of 6th Annual ACM/IEEE Intl Conf on Mobile Computing and Networking (MOBICOM 2000), pages 255–265, 2000.

23. Jonathan P. Bowen , Jonathan Bowen , Jonathan Bowen , Jonathan Bowen , and Victoria Stavridou, "Safety-Critical Systems, Formal Methods and Standards", Software Engineering Journal, 1993.

24. J. Chee, M. Teo, C. How Tan, Energy-Efficient and Scalable Group Key Agreement for Large Ad Hoc Networks, PE-WASUN'05, 114-121, ACM 2005.

25. A. Shajin Nargunam, M.P. Sebastian, Distributed Security Scheme for Mobile Ad Hoc Networks, Proceedings of the 2006 IEEE International Conference on Information Acquisition August 20 - 23, 2006, Weihai, Shandong, China, IEEE.

26. Yanchao Zhang, Wei Liu, Wenjing Lou, and Yuguang Fang, Securing Mobile Ad Hoc Networks with Certificateless Public Keys, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 3, NO. 4, 2006

27. Hengjun Wang, Yadi Wang, Jihong Han, A Security Architecture for Tactical Mobile Ad hoc Networks, Second International Workshop on Knowledge Discovery and Data Mining, IEEE Computer Society, 2009.

28. G. A. Safdar, C. McGrath, M. McLoone, Limitations of Existing Wireless Networks Authentication and Key Management Techniques for MANETs, Proceedings of the Seventh IEEE International Symposium on Computer Networks (ISCN'06), IEEE Computer Society, 2006.