Performance Analysis of Enhanced Ad-Hoc on-Demand Distance Vector Routing Protocol in Smart Environment

Munisha Devi, Nasib Singh Gill

Abstract*: MANETs have specific features that can satisfy the mobility and heterogeneous requirement of the smart environment. Smart applications need high Mobility, Bandwidth, Reliability and less Packet Loss and Delays; therefore, it is important to provide good Quality of Service (QoS) in such applications. So there is a dire need of identifying and exploring the relevant protocols that may be adapted for IoT enabled the smart environment. The routing protocols in smart environments are accountable for connectivity among nodes, fairness, quality of service, etc. Protocol & path selection is the main strategies to design any mobile network. The chosen protocol must have the best in term of data integrity and data delivery. Hence the analysis of the protocols become an essential step. This paper presents various securities and safety-related issues of MANET-IoT system, and also advocate the requirement of enhancing routing protocols in a smart environment. In this research, a new enhanced cache update technique is introduced in MANET protocol to make it enable for the upcoming smart environment. The enhanced algorithm helps to detect the malicious node and remove the stale route present in the network, no matter which traffic mode is used and in which direction nodes are moving. Cache is upgraded in such manner that all nodes in the way are notified about the misbehaving node and its adjacent neighbors' nodes will not use misbehaving node while searching for the route. Here the analysis has been done taking a various number of nodes. Packet Delivery and Packet Lost are two key parameters taken for analysis purpose.

Index Terms*: AODV, *IoT Applications, MANET, Routing Protocol, Security Requirements, Smart City.

I. INTRODUCTION

The smart environment provides a smart solution and provides a good quality of life to its citizens. It provides a society that is invisibly and richly interwoven with displays, actuators, sensors, embedded seamlessly in everyday things to our lives and provides a sustainable and clean environment. Significant growth in communication technologies has led to smart environment things/ objects to interact with each other while ensuring network connectivity. However, these communication technologies can't provide flawless connectivity in the smart environment due to the emergence of millions of devices due to their heterogeneity and distinct behavior, which pose different, kinds of challenges. The smart environment is a combination of IoT and MANET technologies. The interaction between MANET with IoT (Internet of Things) creates a new MANET-IoT system. These systems provide better mobility for users and reduce the implementing costs of the network. IoT is a promising technology in today's modern n age. This technology increases rapidly as an auspicious trend towards connecting physical gadgets. Basically, IoT provides a scheme so that the deva ices can be intermingled together or with end users by organizing a system of related things [1]. Along with easy-deployable MANET and low-cost WSN, the smart environment offers new opportunities. The current improvements in the MANET help to communicate without the energetic creation and pre-defined setup of the network, joining several IoT based presentation domains in smart town's displays large wins. Internet of Things and Ubiquitous Computing are a promising technology in the modern age and therefore it is compulsory to provide a high-level security mechanism for such advanced Technologies. Many people in the world use the internet for different purposes like accessing social networking sites, animation, online games, downloading videos and audios files, emailing extra. MANET has the ability to set up a network during the short-term and crisis period without any infrastructure. Unification of MANET and IoT will surely provide better results in a real context. A huge number of emerging application areas are utilizing constrained devices in a heterogeneous sensor network. One such area is the smart environment (Internet of Things) which enables various resource constraints devices to communicate in the network. Limited memory, low power, limited processing ability, and low-performance cost is a limitation to these devices. The smart environment demands high privacy and data security in sensor network where a large number of sensor nodes are communicating their private data. And this is possible through developing efficient MANET routing protocols in a smart environment. A number of low cost and low energy sensor nodes are involved in Wireless Sensor Networks (WSNs). These nodes communicate via wireless links at a short distance. For such a platform, regular algorithms may incur very high power consumption. Sensor networks connect numerous sensors to a central hub. Batteries or solar panels run these sensors. To provide high security and privacy, secure solutions must be used.

Revised Manuscript Received on July 06, 2019.

Munisha Devi, Department of Computer Science and Applications, Maharshi Dayanand University, Rohtak, Haryana (India).
Nasib Singh Gill, Department of Computer Science and Applications, Maharshi Dayanand University, Rohtak, Haryana (India).

II. LITERATURE SURVEY

Prompt interaction and communication among smart devices have been achieved in a highly dynamic and mobile environment. And all this has only been possible due to the emergence of MANET equipped IoT technology. Handshaking of IoT and MANETs play an important role in many advanced and challenging application like monitoring and logistics, controlling, traffic management, smart cities, etc. Authors in [2] reported that MANET can be considered as a self-arranged and self-organized class of mobile nodes in a dynamic network. Wireless Sensor Network and MANET are the main bases for smart cities and IoT applications. An enhanced solution is given in [3] to put together the collaborative network construction of WSN and the MANET on-demand network development skills for smart area information excavating in a smart environment. A smart home system based on DSDV and AODV protocols in MANET are shown paper [4]. Jitendra Pandey et al. [5] presented a new scheme to heal the link failure problem in routing. And presented mobile power aware stable nodes for the smart environment and they have proposed a self-healing structure for smart city network. Authors have modified AODV to fix the network protocol. Virtual nodes concept has been used. Virtual nodes help in reconstruction phase by the quick selection of a new route. The power conditions of the nodes considered to be available to select virtual nodes. Information about members of virtual nodes and power status is maintained by the individual route tables. When a new route is required, the condition of power is checked and the path is established. When link rupture is detected the node does broadcast a hope data to the adjacent neighbor. The link disconnection information is specified by the data header node and request has been made for the alternate routing. Once the data is received the alternate route is created through the virtual nodes by checking stability and power conditions and the last one hope neighbor route initiates the maintenance phase. For simulation and NS 2.34 has been used. Plans have been created for both UDP and TCP with a similar number of connections. Authors in [6] said that a smart environment provides an innovative way of managing different components like buildings, homes, health, transportation, etc. Effective data management requires new techniques and methods to produce information that is important in utilizing and management of resources intelligently and dynamically. A multi-level architecture of smart environment has also been presented by the authors that were inspired by semantic web technologies and Dumpster Shafer uncertainty. According to Villanovan [7], MANETs are useful in a home environment like an office, buildings, hospitals, etc. Smart building networks are quality of service architecture oriented framework which is adaptive and context-aware. The effect of various packet dropping attacks (Great hole, Blackhole, Selfish) in MANET is shown in the paper [8]. The result showed that such packet dropping attacks have adverse effects on the performance of the T-MANET protocol, and it can worsen in a highly dynamic environment. Attacks cause more energy consumption, the higher end to end delay and more packet drop with less output. In paper [9] authors discussed various techniques for secure routing in IoT devices for the mobile ad-hoc network. They have mentioned various research challenges in this field. Thebig. Mnoorul [10] has done an analysis of various protocols in MANET and IoT. In paper [11] various routing schemes have been categorized according to On-Demand and Table Driving Strategies and comparison have been drawn. On the basis of this comparison, we can easily conclude in which situation, which protocol is suited and MANET and IoT enabled smart environment is also discussed here. In paper [12] an extensive literature survey is done by authors to identify the various gaps of present MANET protocols and shown the basic security requirement. They have drawn attention towards protocol enhancement requirement in the network and showed that up to now most of the work is done in a small area. Paper [13] presented the route cache update technique. Various quality of service parameters was taken for evaluation. And the new technique has improved the performance of dynamic source routing protocol up to 30 percentage. In [14] the author proposed a new EDSR protocol for MANET. And implementation works showed the performance by taking less number of nodes in the network and showed as the number of nodes increases performance decreases. They discussed the problem of Energy Efficiency while designing the routing protocols. In [15] authors evaluated the role of MANET in IoT. They have taken a case scenario for the smart environment. Within their article, they offered MANET state-of-art review, radio frequency identification, near field communication, wireless sensor Network, and protocols as a mean to show their applicability towards IoT. In [16] authors proposed the technique of safe- weighted clustering routing and Energy Efficiency for an internet of things system using the interaction of WSN and MANET routing principles.

III. SECURITY PROCEDURES

The security aspect of IoT is a major challenging issue because lots of different objects are networked and organized here. Research shows that IoT network may have lots of attacks like Denial-of-Service, Android Malware, Spam, Web-Based Malware and the others attack. Hence there is a need to develop a protected structure for data transmission [17]. Validity, accessibility, and non-repudiation are the primary conditions of the wireless network framework. Confidentiality is a key parameter that ensures that our information reaches the right source. Honesty is also one of the main features of security. Scheming safe and enabled routing protocols for MANET is the main function, but the network pathway is very important in preserving evidence and security. Different authentic practices are used to provide protection for routing material during transmissions. During hope to hope conduction, security protocols are surrounded by a routing mechanism to confirm and authenticate packets.

All intermediate nodes are necessary to complete and verify the digital signature attached to the dispatch packets. IoT network system used in combat fields uses various MANET techniques for communication [18]. Figure 1 specifies the dependency on the security functions implemented at the connection point of MANET and IoT. The high-security mechanism should be used on these junction points to investigate cyber-attacks and therefore preparing good routing protocols is necessary for the interactive MANET system [19].

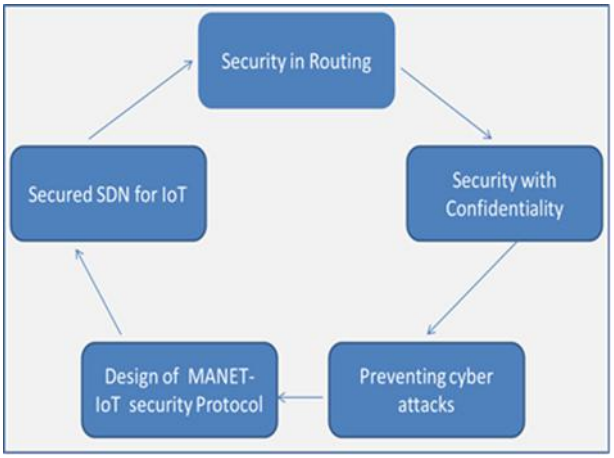

Figure 1: Interdependence Security features in IoT & MANET

IV. THE REQUIREMENT OF ENHANCING ROUTING PROTOCOLS IN SMART ENVIRONMENT

We have observed some limitations in existing MANET routing protocols [12] [20]. Reducing the routing protocols problems will develop a secure, efficient and better application in a smart environment.

- Most of the existing MANET protocols forward hello packets or acknowledgment between nodes which enhances the delay and load on the system.
- Most of the routing protocols are unable to find the optimal path between sources to a destination.
- Link reliability is not concerned at all, such as node battery lifetime, loads delay, bandwidth, etc. and hence these routes are not sufficient for data delivery between source to the goal node.
- They exert more loads on the node in terms of power consumption, processing power, and memory size.
- Only one path is defined, however, if, the main part fails then protocol requires another path, which will consume extra cost, power and time.
- They try to choose the shortest route from initial to the goal node, but when the shortest route is congested at that time there should be some mechanism to choose the longer but efficient route.
- Existing routing protocol not covers all problems such as delay, data drop, more overhead, etc.
- The issue of adaptation according to dynamically changing topology [11].

Some "Should Have" Features of Routing Protocols in Smart Network are shown below:

- When locating a route between initial to the goal node, various Quality of Service parameters such as node battery life, delay, data rate should be considered.
- While changing topology, there should be minimal overhead.
- When the path gets invalid, there should be some mechanism to provide the quick establishment of a path in the system.
- Consider the optimal path instead of the shortest route when an application needs quality of service such as packet Losses, an end to end delay, bandwidth, etc. to send packets from initial to the goal node.
- There should be a mechanism which automatically finds another way to send packets when the primary path fails during the changing topology.
- Develop protocols, which are capable to handle high mobility conditions.
- The routing protocol may need to implement security to protect against attack.

Enhancements should be done in such a way that the protocol can fix routing if the link fails. Based on the concept of self-treatment, the technology will help in creating an adaptive system, which provides functionality despite the possibility of disaster [21].

V. AD HOC ON-DEMAND DISTANCE VECTOR ROUTING IN SMART ENVIRONMENT

MANET is a special type of wireless network in a smart environment. It does not have any infrastructure or base station. Every node is acting as a router. If any node wants to send data to somebody, it receives the data and forwards like a router. This type of networks is used in emergencies cases, where we cannot go for constructing any fixed infrastructure [22]. In MANET, routing is a difficult task. The basic two types of routing are Proactive and Reactive routing. In proactive, every node keeps on updating its own routing tables regularly at a periodic interval. The benefit is that the routing table shows the latest information but the major disadvantage is all the nodes are battery operated, a battery of every individual node is wasted even though there is no data transfer. In reactive protocols, Route Discovery process starts only when it needs to send data [23]. AODV protocol is reactive routing protocol, designed to control the bandwidth used by data utilized in MANET, by preventing the periodically updating packets used in the proactive routing protocol. This protocol provides self-starting, dynamic and multi-hop routing in the network [24]. This only search the way when it has to send data. The purpose of this protocol is to reduce the traffic overload. It detects route whenever necessary and needed. It enables mobile nodes to respond to link breakages in the system in a timely manner.

Here nodes do not contain any information of neighbor nodes and they work separately. Instead, all nodes contain information about the predefined path through which data can be sent to the target node. Route creation and maintenance are two important steps here. When a node needs to transmit a packet, it first checks the routing table, whether the valid & fresh path is available or not. If a path is available, then RREQ (Route request) is transmitted to all neighbors. RREQ received by all its neighbors. Every node whoever receives the route request message does few things, first it check whether the ID is new or not, if it is new then neighbors node check whether the destination address matches with its own address or not, if it matches then it give reply, if the address does not match & RREQ is new message then broadcast that message further that is called flooding. This protocol maintains a sequence number for a fresh route and keeps table entries according to fresh route information [25]. The main difference between DSR and AODV is that in AODV, the source node & the middle node will store the next hop information but in DSR every outgoing packet will have complete route information from the source to the destination.

VI. PROPOSED ALGORITHM

The cache route concept is used by the On-Demand Routing Protocol to make routing decisions, but generally, these routes become stale due to node mobility in the network. Packets are often lost through stale routes. The surrounding nodes get easily corrupted by the malicious node and therefore we are enhancing the basic AODV algorithm. The algorithm consists of two phases: 1) Route Discovery 2) Detection of malicious node & routing table update algorithm.

A. Route Discovery algorithm (Sx, Ix, Dx)

- Designate the Source node as ‘ Sx’ , Intermediate node as ‘ Ix’ , Destination node as ‘ Dx’ .
- RREQ is forwarded as source routing. AODV protocol is followed.
- If ‘ Sx’ is equal to ‘ Dx’ we return "success".
- Else node ‘ Sx’ will broadcast the message to all neighbors and get load and response time.
- Search node with less cost and less load called that node ‘ Ix’ .
- If Reply status of ‘ Ix’ is "true" we set it as the current node and route is established.

B. Detection of malicious node & table update algorithm

- Set Delay Period (d) of mobile host = C*(H-1+n), Where C is a small constant delay, 'H' provide the number of hops need to deliver data and n is a random number from 0 to 1.
- If a node sends data after a delay time, that particular node fails & is temporarily blocked. The number of hops replied the host has less length than a requirement.
- Misbehaving node (In) is either in terms of a broken link or in case of an attack on it.
- Node ‘ Jm’ detect the failure node and request to block this node.
- Routing table entries are updated and Reply status of the misbehaving node is set as "No" so the neighbor’ s node does not use it as a part of the network.

If a node does not deliver data within hop time, the node will be treated like a misbehaving node and it will have a low packet delivery ratio and high packet drop rate. And this misbehaving node is temporarily blocked. Each node keeps the necessary information for cache updates in the cache table. Tables are upgraded in such manner that all nodes in the way are notified about the misbehaving node and its adjacent neighbors’ nodes will not use misbehaving node while searching for the route.

VII. EXPERIMENTAL RESULTS AND ANALYSIS

We carried out a simulation on mobile Ad Hoc Network by using ns2. It gives a highly modular platform for wireless and wired simulations supporting different routing types, traffic, protocols, network elements. It contains the NAM (network animator) tool. NAM is used for visualization. Trace graph tool is used for plotting graph & it is supported by Mac OS, UNIX, and Linux.

Packet Delivery Ratio: It is the ratio of the total received packets by the receiver, to the total sent packet by the sender. It shows the correctness and completeness of the routing protocol.

Packet lost Ratio: The ratio of total lost packets to total sent packets.

Simulation Parameters	Values
Ns-2 Version	ns-2.35
Network Type	Wireless
Routing Protocol	AODV
Number of Nodes	25,50
Antenna Model	Antenna/OmniAntenna
Mac Type	802.11
Traffic Agent	CBR
link layer type	LL
Propagation Mode	TwoRayGround
Environment Size	800*800
Interface queue	Queue/DropTail/PriQueue
Mobility Model	Random Waypoint Model

The graph for 25 nodes

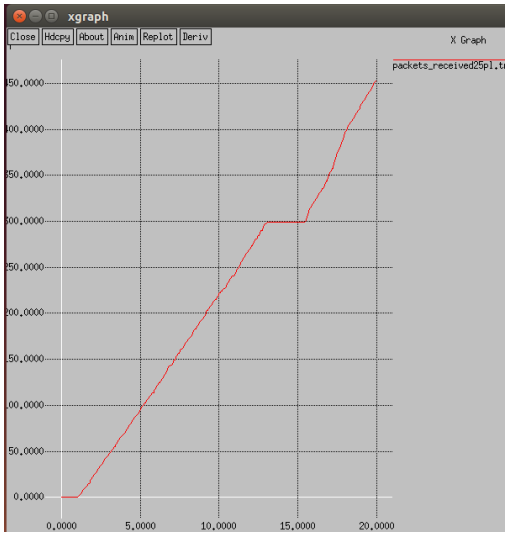

Fig 2 shows Packet received for 25 nodes of Enhance AODV

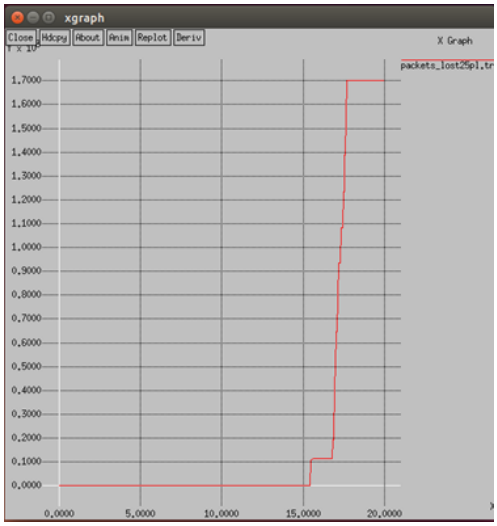

Fig 3 Shows packet lost for25 nodes of the Enhance AODV

2. The graph for 50 nodes

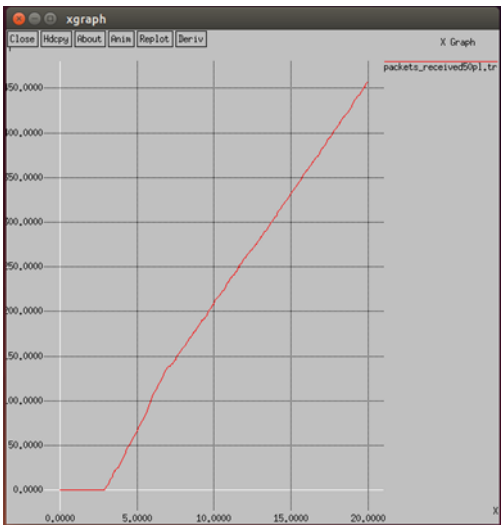

Fig 4 shows packet received for 50 nodes of the Enhance AODV

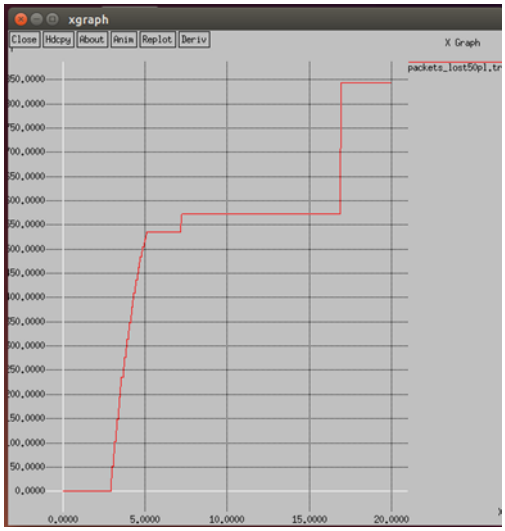

Fig 5 shows packet lost for 50 nodes of the Enhance AODV

Comparison Graph

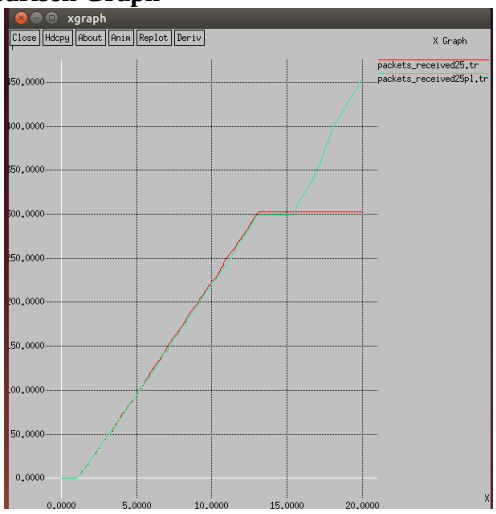

Fig 6 shows the comparison for Packet Received for 25 Nodes with Basic AODV and Enhance AODV

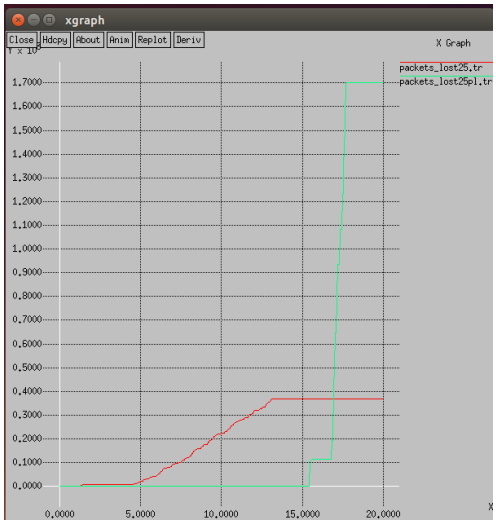

Fig 7 shows a comparison of Packet lost for 25 Nodes with Basic AODV and Enhance AODV

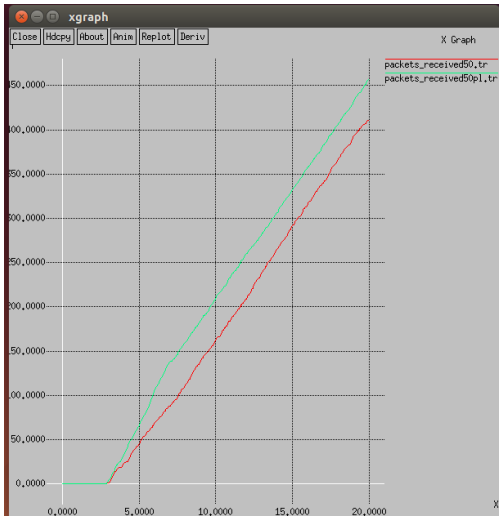

Fig 8 shows a comparison of Packet Received for50 Nodes with Basic AODV and Enhance AODV

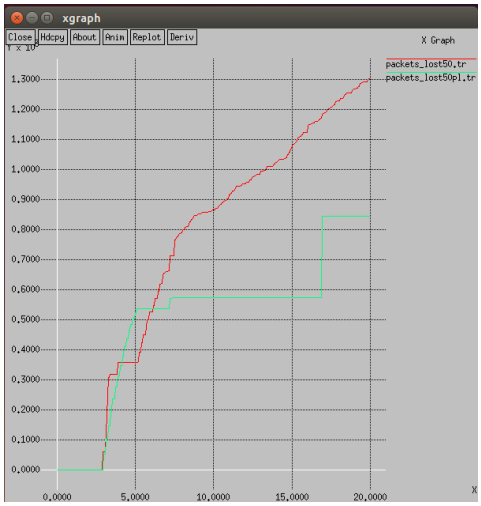

Fig 9 shows a comparison of Packet lost for 50 Nodes with Basic AODV and Enhance AODV

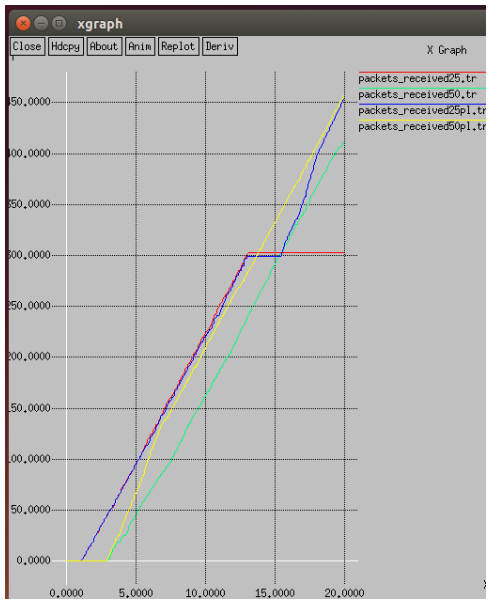

Fig 10 shows packet received for 25, 50, nodes of the basic AODV and enhance AODV

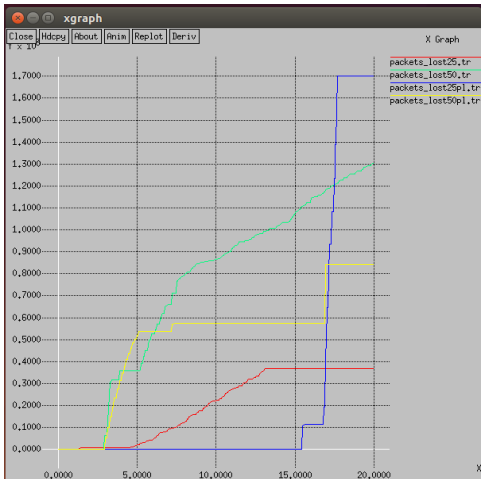

Fig 11 shows packet lost for 25, 50, nodes of the basic AODV and enhance AODV

VIII. CONCLUSION

Reducing the Routing Protocols problems will develop a secure, efficient and better application in a smart environment. In this context, a thorough study and analysis have been done about the safety aspects of IoT- MANET technology. With this kind of analysis, the requirement for the development of more intelligent, challenging and secure routing protocols on the intersection of Lot and MANETs will definitely be encouraged. After extensive literature survey, we realized that there are lots of security problems like Packet Loss, Frequent Disconnection, Short Battery Lifetime, More Overhead, Issue of Adaptation, Power Consumption Problem, Security Implementation, etc. We have to develop such protocols that allow sufficient coupling between devices and on the other hand are extremely efficient in the use of communication. We have presented the requirements for enhancing routing protocols in a smart environment. We have introduced a new enhanced cache update technique in MANET. The technique enables AODV to adapt according to topology changes. It reduces the packet drop ratio and improves the packet delivery ratio in the network. The enhanced algorithm helps to detect the malicious node and remove the stale route present in the network.

REFERENCES

1. N. Shahid, and S. Aneja, “Internet of Things: Vision, application areas and research challenges”. *Proceedings of the International Conference on IoT in Social, Mobile, Analytics, and Cloud, I-SMAC* 2017, 10(7), 583–587.2017. https://doi.org/10.1109/ISMAC.2017.805826.
2. C. Sandhiya, “An overview on Wireless Sensor Networks and Mobile Ad Hoc Network”. *International Journal of Engineering Science Invention*, (2018), 10-14.
3. P. Bellavista, G. Cardone, A. Corradi, and L.Foschini, “Convergence of MANET and WSN in IoT urban scenarios”. *IEEE Sensors Journal*, 13(10), (2013), 3558–3567. https://doi.o.rg/10.1109/JSEN.2013.2272099.
4. O. A. Mohamad, “Smart Home System Based on Comparative Analysis among AODV and DSDV Protocols in MANET”. *19th International Conference on System Theory, Control, and Computing (ICSTCC), October 14-16, Cheile Gradistei, Romania*, (2015), 687–692.

5. J. Pandey, A. Kush, and R. Al. Ababseh, "Novel scheme to heal MANET in smart city network".*3rd MEC International Conference on Big Data and Smart City, ICBDSC* (2016), 34–39. https://doi.org/10.1109/ICBDSC.2016.7460339.
6. A. Gaur, B. Scotney, G.Parr, and S. McClean, "Smart city architecture and its applications based on IoT". *Procedia Computer Science*, 52(1), (2015), 1089–1094. https://doi.org/10.1016/j.procs.2015. 05.122.
7. F. J. Villanueva, D. Villa, F. Moya, J. Barba, F. Rincon, and J. C. Lopez, "Context-aware QoS provision for mobile ad-hoc network-based ambient intelligent environments". *Journal of Universal Computer Science*, 12(3), (2006), 315–327.
8. A. M. Shabut, K. Dahal, M. S. Kaiser, and M. A. Hossain, "Malicious Insider Threats in Tactical MANET: The Performance Analysis of DSR Routing Protocol". *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, Things-Green Com-CPS Com-Smart Data* 2017, 2018, 390–395. https://doi.org/10.1109/iThings-GreenCom-CPSCom-Smart Data.2017.64.
9. J. Karlsson, L. S. Dooley, and G. Pulkkis, "Secure Routing for MANET Connected Internet of Things Systems". *IEEE 6th International Conference on Future Internet of Things and Cloud (Fi Cloud)*, (2018), 114–119. https://doi.org/10.1109/FiCloud.2018.00024.
10. A. Jangra, and Meenakshi, "An Analysis on Routing Protocols for the Internet of Things". *International Journal of Advanced Research in Computer Science and Software Engineering*, 7(5), (2017), 754–756. https://doi.org/10.23956/ijarcsse/V7I5/0117.
11. M. Devi, and N. S. Gill, "Mobile Ad Hoc Networks and Routing Protocols in IoT Enabled Smart Environment: A Review". *Journal of Engineering and Applied Sciences*, 14(3), (2019), 802-811.
12. M. Devi, and N. S. Gill, "Study of Mobile Ad hoc Network Routing Protocols in Smart Environment". *International Journal of Applied Engineering Research*, 13(16), (2018), 12968–12975.
13. V. V. Mandhare, & R. C. Thool, "Improving QoS of Mobile Ad-hoc Network Using Cache Update Scheme in Dynamic Source Routing Protocol". *Procedia Computer Science*, 79, (2016), 692–699. https://doi.org/10.1016/j.procs.2016.03.090.
14. P.A. Madnaik, "Enhanced DSR An Efficient Routing Protocol For MANET". *International Journal of Engineering Sciences & Research Technology*, 7(8), (2018), 349–354.
15. G. Reina Daniel and L. Toral Sergio, "The Role of Ad Hoc Networks in the Internet of Things: A Case Scenario for Smart Environments", *Chapter, Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence*, Vol 460, Pages 89-113, ISBN: 978-3-642-34951-5 (Print) 978-3-642-34952-2 (Online)-2013.
16. R. Bruzgiene, and L. (n.d.) Narbutaite, *World ' s largest Science, Technology & Medicine Open Access book publisher MANET Network in the Internet of Things System*,2017.
17. D. Airehrour David, "An analysis of secure MANET routing features to maintain confidentiality and integrity in IoT Routing". http://www. Research gate. Net/ publication/277078202, last accessed on - August 2015.
18. Z. Hua, "A Password-Based Secure Communication Scheme in Battlefields for the Internet of Things". *China Communications*, Vol.8, (1), (2011) Pages 72-78.
19. J. Karlsson, L. S. Dooley, and G. Pulkkis, "Secure Routing for MANET Connected Internet of Things Systems". 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), (2018), 114–119. https://doi.org/10.1109/FiCloud.2018.00024.
20. Poonam, K. Garg, and M. Misra, "Trust-based security in MANET routing protocols". *Proceedings of the 1st Amrita ACM-W Celebration on Women in Computing in India - A2CWiC* '10, (2010), 1–7. https://doi.org/10.1145/1858378.1858425
21. I. A. Alameri, "MANETS and Internet of Things : The Development of a Data Routing Algorithm", *Engineering, Technology & Applied Science Research*, 8(1), (2018). 2604–2608.
22. M. Tsujimoto, H. Shimizu, C. Nishigori, and G. Tsuji, "A case of systemic plasma cytosis improved by the treatment with mizoribine". *Skin Research*, 11(2), (2012). 173–178. https://doi.org/10.1016/S1570-8705 (03)00013-1.
23. A. Bouroumine, M. Zekraoui, and M. Abdelilah, "Enhancement to the Ad-hoc On-demand Distance Vector routing protocol for vehicular communications in a Smart City". *Proceedings - 2016 International Conference on Wireless Networks and Mobile Communications, WINCOM 2016: Green Communications and Networking, (2016).* 214–219. https://doi.org/10.1109/WINCOM.2016.7777216
24. B. Sachdeva, "Multilingual Evaluation of the DSR, DSDV and AODV Routing Protocols in Mobile Ad Hoc Networks". *Proc. IEEE Conference on Emerging Devices and Smart Systems (ICEDSS 2017) 3-4 March 2017, Mahindra Engineering College, Tamilnadu, India*,1(3), (2013),51–57.
25. M. N. Abdulleh, S. Yussof, and H. S. Jassim, "Comparative Study of Proactive, Reactive and Geographical MANET Routing Protocols". *Communications and Network*, 2015, 7, 125-137 (2015), 125–137. http://dx.doi.org/10.4236/cn.2015.72012G.

AUTHORS PROFILE

Ms. Munisha has passed Master of Technology from Maharshi Dayanand University, Haryana, India in 2014. She is currently pursuing Ph. D under the supervision of renowned academician and researcher – Professor Nasib Singh Gill of M. D. University. She has published more than 15 research papers in reputed National and International Journals and Conference Proceedings including IEEE. Her main research work focuses on MANETs, IoT, Network Security and Privacy, Big Data Analytics and Data Mining.

Dr. Nasib Singh Gill is at present senior most Professor of Department of Computer Science & Applications, M. D. University, Rohtak, India and is working in the Department since 1990. He has earned his Doctorate in Computer Science in the year 1996 and carried out his Post-Doctoral research at Brunel University, West London during 2001-2002. He is a recipient of Commonwealth Fellowship Award of British Government for the Year 2001. Besides, he also has earned his MBA degree. He has published more than 260 research papers in reputed National & International Journals, Conference Proceedings, Bulletins, Edited Books, and Newspapers. He has authored seven books. He is a Senior Member of IACSIT as well as a fellow of several professional bodies including IETE and CSI. He has been serving as Editorial Board Member, Guest Editor, Reviewer of International/National Journals and a Member of Technical Committee of several International/National Conferences. He has guided so far 8 Ph.D. scholars as well as guiding about 7 more scholars presently in the areas – IoT, Information and Network Security, Computer Networks, Measurement of Component-based Systems, Complexity of Software Systems, Decision Trees, Component-based Testing, Data mining & Data warehousing, and NLP.