Novel Algorithm for Enhancing MANET Protocol in Smart Environment

Munisha Devi and Nasib Singh Gill

Abstract: ***Future smart environment will consist of smart devices (objects) that will form an autonomous and distributed ad-hoc network near the user end. This network needs efficient, cooperative and effective protocols for the changing network. So it requires a flexible and unified framework for wireless intelligent devices communication that will permit secure and adaptive routing to fulfill ad-hoc networking requirements. It is important to propose effective protocols and to identify good architecture for the future internet. Active routing protocols update the table of information on a regular basis and keep the mobility factor in control. The result of routing optimization with an efficient and effective scheme to mobility control and energy consumption in MANET-IoT system shows the main solution of Smart Network. Combination of IoT and MANET routing mechanism enhances the lifetime of nodes in the overall smart environment. This combination helps in the provision of services and accessibility for a longer period of time over the future smart environment. 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 paper, a new algorithm has been developed to reduce the delay factor of MANET protocol in a smart environment and performance is evaluated between the existing and proposed approach on the active protocol.***

Index Terms: ***Smart environment, IoT applications; security requirements; smart city, MANET, IoT, Routing Protocol, AODV.***

I. INTRODUCTION

The internet is one of the most important and transforming technology ever invented. Internet is like a digital fabric that affects our life in one way or others. The internet of people changed the world but there is a new internet emerging which is about connecting things and so its name is the internet of things (IoT), here the things share their experience and communicate with one another [1]. It is like take things and add sense and communication power to them. Here the things interact and collaborate with other things. For example our smartphone, it has many sensors, it knows where we are, it knows what we are saying to it (through Google), it knows how close it is to our face, it knows how much light around us, it knows how we are holding it, it knows if we are moving, even it has an eye (camera) so it can see our surroundings and has the power to communicate in a wireless and mobile network. Smart devices learn and track pattern to ensure our comfort and save energy and it communicates in the network and we can control them. Because they can communicate in the network so they know how to listen, we can tell them or other smart things can tell them to turn on, off or play. We can take the example "armband". If we have armband on our hand during night, it senses the sleep cycle and know when to wake up people by gently vibrating and blinking light with the same time send message to other smart things at home and a chain of event starts, because now things are talking to one another for example, house fan startup and draw all the morning air in the house, which cools the home and coffee maker starts up automatically etc. We all want to live a better life and technology like IoT has the ability to sense, communicate and provide new levels of comfort for us. It is a perfect technology to collect raw data and turn it into knowledge and then wisdom and move the human race forward. Technology is accelerating force. The smart things can send information in MANET across all active things without any centralized scheme [2]. The mobile (sensor) network is the backbone of smart environment. The smart things act as router under the IoT environment. In the Smart World ahead, we will see how physical things will be able to automatically exchange data among themselves. IoT (Internet of things) is a technology that facilitates the interlinking of physical things with the digital world. MANET is a set of nodes, which are basically distributed spatially and communicating each other wirelessly and here smart things can communicate with each other remotely. Every intelligent gadget is able to change its location by using the MANET mobility feature. The MANET in IoT is a combination of portable autonomous smart things that can transfer data to each other through a wireless network. Safety emergency requires quick and clear communication. Emergency medical technician, Fireman, a Police officer, and dispatch team all rely heavily on the mobile communication system and if tragedy strikes in rebel area, the current wireless communication technology is not always available, when it is available it is not reliable or fast enough, especially for time sharing sensitive information. So how can we improve the wireless mobile network to help first responders? We need to develop a new protocol or a new scheme that can eliminate unnecessary communication between devices, so by eliminating this overhead they can actually forward the data in a timely manner without incurring any penalty, where each node can make its decision locally, and then mobility would not be a problem. We

Revised Manuscript Received on August 05, 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).

should develop Technology for public safety and first responders deployed in the area. Where there is no cellular coverage or even if there is a cellular coverage in cases of disasters and catastrophic, then that network can be highly congested. So in that case, the ad-hoc mobile Technologies comes in handy. Our vision should be to develop some wireless devices such as "helmet-mounted camera" streaming live video for the rescue team along with "wrist-mounted touch screen watch" streaming data across the team. Technologies playing a vital role in the case of HD video transmission and emergency response communication. One example of a safety emergency is road accidents. Road accidents illustrate a major issue and one of the main cause of death. Most of the road accidents due to human error and 70% of this accident could have been stop if the driver had been worn at least half a second beforehand. Here, VANET is established to minimize the risk of road accidents and to maximize passengers comfort by permitting automobile to exchange various kind of information. The safety-related applications and MANET protocols represent the main objective of communication when the accident occurs, a vehicle can continuously broadcast data about this critical situation to the approaching vehicles. When a vehicle brakes suddenly, it send data about its current status, which is used by surrounding vehicles to quickly detect the sudden breaking and to strengthen the quality of service requirement and efficient routing protocol that can give a broadcast service with bounded access delays and low transmissions collisions are needed. A new Mobile Network should be there to support issues related to IDM with several personal attributes and mobility. So we can say that mobile ad hoc network protocols can play a major role during communication in this network. MANET-IoT Internet concept shown in the below figure [3].

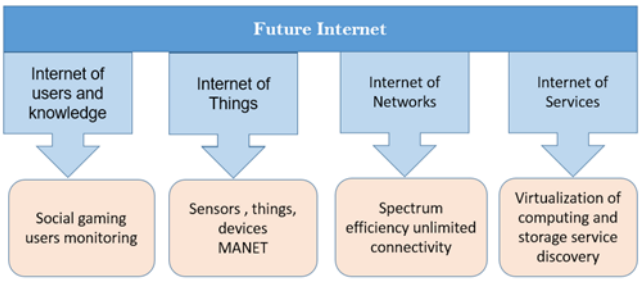

Fig1: MANET-IoT Internet concept

IoT has a pool of MANET autonomous portable devices that can communicate information to each other via WiFi waves. Communication is easy for those smart devices, which are in each other's Wi-Fi range. Whereas other devices need some intermediate intelligent device to convey their data packets. Link is built in real time, which separates the whole network and can work anywhere without the help of any access point.

II. LITERATURE SURVEY

In the paper [4] the author described the integrated scheme of MANET and IoT using clustering approach to balance the energy on smart things because the IoT nodes behave like a smart object and sometimes behave as a router in the mobile network. Authors in [5] concentrate on efficient energy consumption in MANET-IoT framework.

In the paper [6] fuzzy controls communication system is used for the presentation of MANET framework. Here the MANET mobility model has been presented by the authors for the performance evaluation of MANET in IoT network. Authors in [7] describe the requirement of protocols in MANET-IoT system. In paper [8] authors describe a new blockchain system in IoT network. The blockchain purpose was to secure and authenticate the data taken from smart things of the IoT system. The author in [9] has given attention to the various challenges in MANET-IoT connectivity and discussed the requirements of new security protocols in the network.

In [10] Probabilistic model is presented by the authors for the evaluation of smart things in the network. A Probabilistic Model is represented in a mobile network to track the smart devices in the system. Its sense or detects the target device during moving the cell of the system where the sender is present. The data is created in a transmitted manner which uses the weighted angle. The angle is given by IoT device versatility, and smart device experiencing the aim spares the aim area and sets the inclination to be on that plunges and it becomes more seasoned.

Authors in [11] represented a model for MANET-IoT system, this model performs better in the large-scale network. But it had security issues. Communication in IoT- MANET network is presented by jony karlsson et.al [9]. They presented communication options for IoT devices connected to MANET. For example, an IoT device can be a MANET node or it can be connected to a MANET node, and either it can be an internet node or connected to an internet node. An IoT device which is a MANET node or connected to a MANET node can communicate with IoT devices connected to the same or other MANET node or with cross MANET over internet-connected IoT device and so on. Wireless sensors and MANET play a key role in the implementation of IoT system. In MANET, physical quantities such as Light Intensity, Sound Level, Pressure, and Temperature are controlled by sensors and actuators. IoT based smart environment is also discussed in [12]. 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 attacks (Great hole, Blackhole, Selfish) in MANET is shown in the paper [13]. 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 mobile environment. Attacks cause more energy consumption, the higher end to end delay and more packet drop with less output. In paper [14] 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 [15] has done an analysis of various protocols in MANET and IoT. In paper [16] 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 [17] 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 [18] presented the route cache update technique. MANET routing protocols are needed for the routing purpose in IoT devices. So we need to enhance the quality of such MANET protocols.

III. SIMILARITY OF IoT AND WSN

As the name suggested its Wireless (have no wires) Sensors (have a sensor(s)) Network (a network with specific topology). A WSN is a network of small wireless electronic nodes (electronics devices) which consists of a different sensor(s). The purpose of a wireless sensor network is to collect data from these sensors from the subject environment. One most popular topology of this network consists of three types of nodes such as a router, co-coordinator, and end device. There are many popular protocols and devices which perform WSN task one such very popular name is ZigBee Protocol with XBee Devices. WSN is part of an IOT. Sensors need to be connected to an IOT platform via fixed line or 5G mobile network (for a mobile device, such as a car, or person using health sensors). Of course, not each and every sensor will be connected to the platform directly. It is quite natural to use a "local" concentration process, to filter out irrelevant data and correlate data from multiple sensors. That again can be done via some sort of LAN cabling in a bus style or wireless. Here is where you go with WSN.

The Internet of Things in a broad sense is like a brain, it can both store the real world data (in database or cloud) and can monitor the real world parameters, make meaningful interpretation and even make decisions based on the sensed data. IoT is responsible for data processing, manipulation and decision making. IoT combines multiple technologies such as (RFID), wireless sensor networks (WSN), NFC, in fact, WSN is a subset of IoT. For information confidentiality point of view, the existing encryption technology that is used in WSNs can be extended and deployed in IoT. In the other hand, the security protocols that are used by WSN can be integrated as an essential part of IoT security. It should be considered that the security issues, architectures, are different in both IoT and WSN [19].

IV. VULNERABILITIES AND THREATS TO ROUTING IN SMART ENVIRONMENT

The security aspect of IoT is a major challenging issue because lots of different objects are networked and organized here. Various issues are as discussed below [20]:

Mobility of nodes: Nodes and topology were already fixed within the traditional networks but it is not possible to keep the topology and nodes fixed in the mobile network which is the main component of IoT.

Wide-ranging devices: On the basis of network standard used, type of resources, and type of application the devices will get differed. Some devices will have a problem of resource limits and some devices will not.

Fault tolerance: Energy limitations, Positioning of devices are some surrounding factors due to which network performance degrade. To manage this kind of surrounding factors, efficient routing protocol should be proposed.

Various network standards: Here the internet of things combines various approaches like wireless sensor networks, Wi-Fi networks, traditional networks, RFID, Ad Hoc networks, etc. All of these use a different protocol stack. By combining these Technologies we can get a better result.

Research shows that IoT network may have lots of attacks like Denial-of-Service, Android Malware, Spam, Web-Based Malware and the others attack. In MANET, attacks are classified into two categories active and passive attacks. In the first type (active) a malicious node tries to change, disturb, or interrupt the routing functionality of the mobile network. Example of active attacks is Blackhole, Wormhole, Fabrication, Impersonation, and Modification [21]. Passive attack retrieves information or eavesdrops on routing communication. Here a misbehaving node focus to track communication parties and tries to steal their communication details.

Table 1: Possible Attacks in Mobile Network.

Attack	Attack Class	
	Integrity & Confidentiality	***Availability***
Blockhole	no	no
Denial-of-Service		no
Flooding		no
Wormhole	no	
Man-in-the-Middle	no	
Sybil attack	no	
Selective forwarding	no	
Neighbor attack	no	no

We need to develop a protected structure for data transmission. 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. For the detection of malicious node and removal of stale route problem present in the network, we need to identify and explore MANET routing protocols that may be adapted for IoT enabled smart environment [22]. Various mobile nodes in wireless network are shown below.

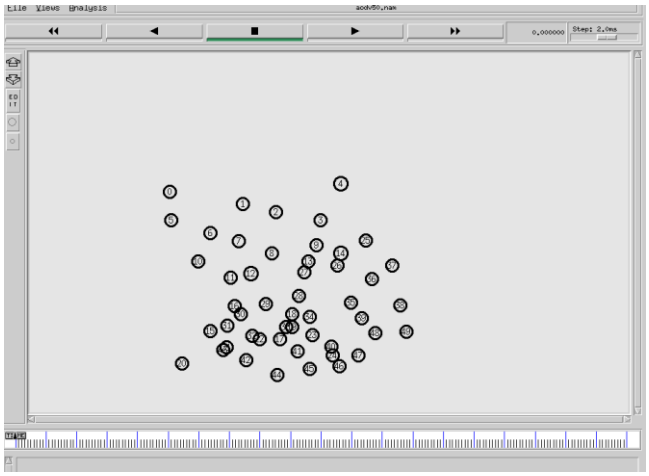

Fig2: Mobile Nodes Distributed Randomly In A Smart Environment

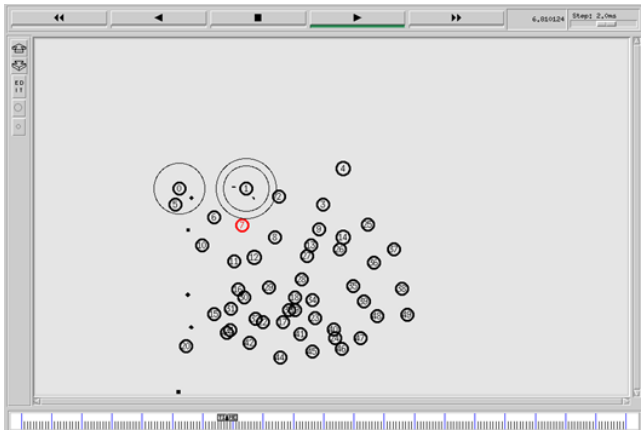

Fig3: Showing The Misbehaving (Red) Nodes Present In The Network

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. These misbehaving nodes do not allow to pass data to the next nodes or we can say that a node with less forwarding ratio is presented as a misbehaving (bad) node. And these misbehaving node should be blocked in the network.

Networking in MANET-IoT system is based on the handling and processing using the internet of things, data sensing from things, routing principles of wireless sensor network and on the routing protocols of MANET. MANET require a less Complex setup processor and has a much wider sequence of operations as compared to typical sensor networks. There are various features of MANET such as shared physical medium, lightweight terminals, dynamic topology, and autonomous terminal, multi-hop routing, and distributed operation.

Routing in WSN aim on the nodes efficient energy consumption and mobile Ad Hoc network protocols all designed with the aim on quality of service. The relation of various devices with limited characteristics to the internet and connection with different mobile ad hoc networks and wireless network must guarantee reliability, accessibility, and connectivity of the MANET-IoT system in a smart environment. The connection of IoT with MANET requires new optimized routing mechanism.

V. PROPOSED WORK

While solving the problem of attack in the network, we cannot ignore the delay factor. Delay is a key parameter while measuring the performance of the ad-hoc network. Delay is the time consumed by the data to reach the target node. Delay in the smart environment gets affected by a number of nodes connected and mobility of nodes present in the network. Our aim is to minimize the value of the delay factor in the mobile network for the active protocol.

Methodology: The delay is measured by taking a large number of nodes. A number of connections and pause time between the nodes (devices) helps to minimize the delay. We have used fuzzy Logic to maintain low delay in the mobile network. The proposed work is about the evaluation of the delay parameter in the mobile network. Intelligent nodes present in the network save the data about neighboring or adjacent nodes and make decisions based on this collected data. Nodes Keep checking whether the adjacent nodes are effectively responding in the system or not. The decision is taken on the basis of delay parameters. Response time of the adjacent node is checked against the expected time and accordingly, exclude the particular node from the network. We also use an algorithm to send the information with true decision making. The whole process is repeated until the target node is not achieved.

Algorithm: To minimize the value of the delay factor in the mobile network for a reactive protocol.

Input: Node parameter

Output: Minimize the Value of Node Parameter (Delay)

Steps:

Step 1: A network is defined with various mobile nodes along with parameter.

Step 2: Design source and destination node as Sx and Dx

Step3: Create route between source and destination respectively using AODV protocol. Set the route as Sx, N1, N2, N3...Nn, Dx.

Step 4: For x=1 to n (repeat steps 4 to 8)

Step 5: NList find adjacent (x)
For y-1 to length (NList)
{

Step 6: Parameter = Packet Delay (y)

Step 7: use of Fuzzy Logic to fuzzify the parameter.
Step 8: If the parameter Delay =low
{
Set Nlist(x) as next communicating node
}
}
Step 9: Move to next node.
Step 10: End

Experimental Results & 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.

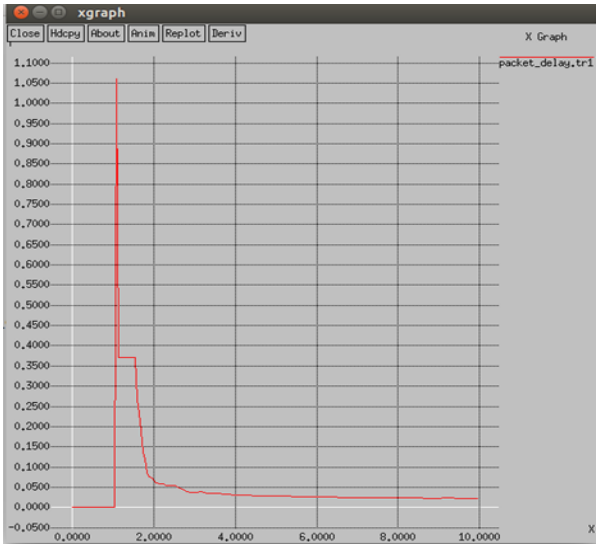

Fig.4: Packet Delay of Existing Approach

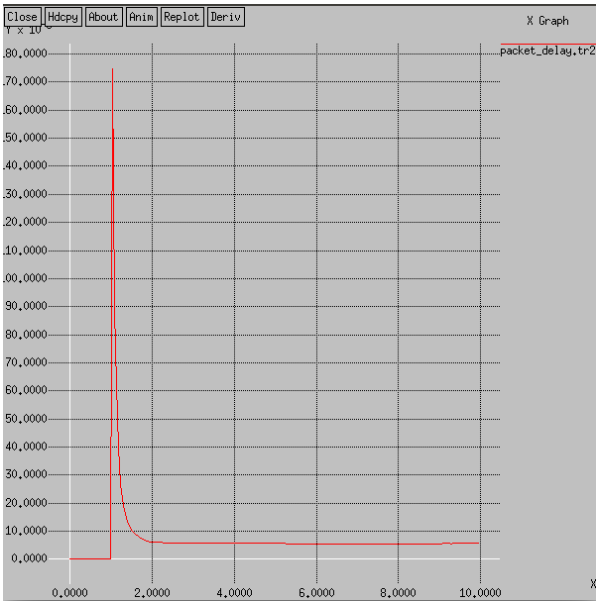

Fig.5: Packet Delay of Proposed Approach

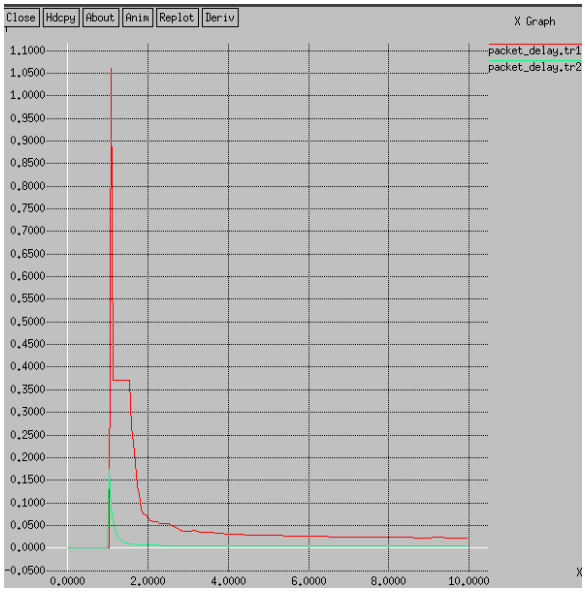

Fig.6: Comparison Of Packet Delay In Both Existing And Proposed Approach

Comparative analysis of packet delay is shown in the above Fig 6. X and Y axis represents the time and delays respectively. As we can see, the delay factor has been reduced after the implementation of the proposed algorithm.

VI. CONCLUSION

Focussing on the protocols has become essential in order to strengthen the smart network. Combination of IoT and MANET routing mechanism enhances the lifetime of nodes in the overall smart environment and such networks may help people especially in a critical situation. After a detailed literature survey, we have learnt as how the MANET works in IoT and what are the benefits of the convergence of MANET with IoT. The proposed work in the present paper is about to minimize the packet delay parameter in the mobile network. Here fuzzy based security system is used to reduce the delay factor in the network. The implementation is done in a mobile network with the AODV protocol. The proposed work may be enhanced in future and may be implemented with some other protocol. Instead of Fuzzy, some other approach like WiMAX and PAN may be used in the future. The proposed algorithm is able to define against active attacks, it would be extended in further for passive attacks too. Future work can be on energy consumption on a large scale in the mobile network. Nodes that are left with low energy or that rapidly lose its energy can be recognized and their workloads can be limited to transactions.

REFERENCES

1. D. Sehrawat, and N. S. Gill. "Deployment of IoT based smart environment: key issues and challenges". International Journal of Engineering and Technology (UAE), Vol. 7, No. 2 pp. 544-550, 2018. ISSN: 2227-524X. http://dx.doi.org/10.14419/ijet.v7i2.9504.
2. P. Bellavista, and G. Cardone. "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.
3. 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.
4. L. Narbutaite, and T. Adomkus. "MANET Network in the Internet of Things System." In Ad Hoc Networks. InTech, 2017.
5. Alameri, I. A. "MANETS, and internet of things: the development of a data routing algorithm." Engineering, Technology & Applied Science Research 8, no. 1 (2018): 2604-2608.
6. T. Alam, "Fuzzy control based mobility framework for evaluating mobility models in MANET of smart devices." ARPN Journal of Engineering and Applied Sciences, 12, no. 15 (2017): 4526-4538.
7. R. Suji Pramila, and N. Islam. "An analysis of routing protocols in MANETs and Internet of things." In IoT and Application (ICIOT), 2017 International Conference on, pp. 1-8. IEEE, 2017.
8. T. Alam, "Blockchain and its Role in the Internet of Things (IoT)", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, pp. 151-157, 2019. DOI: https://doi.org/10.32628/CSEIT195137.
9. 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.
10. N.N. Kachouie, P. Fieguth, J. Ramunas, and E. Jervis. "Probabilistic model-based cell tracking". International Journal of Biomedical Imaging, 2006.
11. Li L., Xu X., Cai Y. (2006) "Gradient-Based Autoconfiguration for Hybrid Mobile Ad Hoc Networks". In: Gerndt M., Kranzlmüller D. (eds) High-Performance Computing and Communications. HPCC 2006. Lecture Notes in Computer Science, vol. 4208. Springer, Berlin, Heidelberg.
12. H. Tahir, A. Kanwer, and M. Junaid, "Internet of Things (IoT): An Overview of Applications and Security Issues Regarding Implementation," Int. J. Multidiscip. Sci. Eng., vol. 7, no. 1, pp. 14–22, 2016.
13. A. M. Shabut, K. Dahal, Kaiser, S. M., 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-SmartData.2017.64
14. M. Devi, and N. S. Gill. "Performance Evaluation of Dynamic Source Routing Protocol in Smart Environment". International Journal of Advanced Trends in Computer Science and Engineering. Volume 8, No.2, March - April 2019. https://doi.org/10.30534/ijatcse/2019/37822019.
15. A. Jangra, & 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.
16. 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.
17. 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.
18. V. V. Mandhare, and 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.
19. H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," In Proc. IEE Wireless Communication, UCLA, Los Angeles, CA, USA; volume- 11, Page(s):38-47, ISSN: 1536-1284.
20. Nishu Garg and R.P.Mahapatra, "MANET Security Issues," IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.
21. Ping Yi, Yue Wu, and Futai Zou and Ning Liu, "A Survey on Security in Wireless Mesh Networks", Proceedings of IETE Technical Review, Vol. 27, Issue 1, Jan-Feb 2010.
22. S.-R. Oh and Y.-G. Kim, "Security Requirements Analysis for the IoT," in 2017 International Conference on Platform Technology and Service (PlatCon), 2017, pp. 1–6.

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.