Constitution of Low-Cost RFID Sensor for Enhancing Security of Hierarchical Mobile Adhoc Network

Mala Kumari[1], Mr. Sudeesh Chouhan[2], Dr. Harsh Lohiya[3]

[1]*Research Scholar, Department of CSE, SSSUTMS, Sehore, Madhya Pradesh, India,*
[2]*Assistant professor, Department of CSE, SSSUTMS, Sehore, Madhya Pradesh, India*
[3]*Assistant professor, Department of CSE, SSSUTMS, Sehore, Madhya Pradesh, India*

ABSTRACT

This particular wireless network is known as a MANET. It's a collection of mobile nodes that doesn't rely on any pre-existing infrastructure to work together. As every mobile node is treated as an intermediate switch, the number of available mobile nodes grows far beyond that of the base transceivers of theirs, thus eliminating the need for a fixed network infrastructure. Because of resource constraints in bandwidth, memory size, battery life, computational power, and unique wireless qualities such as openness to eavesdropping, lack of certain ingress and exit points, increased security threats, vulnerability, unreliable correspondence, and fast alterations in memberships or topologies due to user mobility or even node failure, security protocol designers for MANETs face complex difficulties. Radio Frequency Identification (RFID) engineering is actually replacing barcodes with improved efficiency for identification, tracking, real time monitoring, constant command, localization and also the motion of items. Nevertheless, sensing, mobility as well as long range data interaction is doable via RFID Sensor incorporated products just. This particular effort concentrates on constituting as well as securing inexpensive RFID Sensor integrated hierarchical Mobile Ad hoc Networks (MANET).

A virtual node-based protected hierarchical MANET is actually suggested for providing security in RFID Sensor integrated hierarchical MANET. In fact, both routing and network security are taken into account. According to the performance analysis, the proposed hierarchical MANET has less delay and GEs than the Chen et al. protocol, which is already the best protocol in terms of effectiveness. The proposed system offers a maximum of (0.75)n and a minimum of (0.25)n success probabilities of distance fraud, mafia fraud, and terrorist fraud attacks for two bits challenge based on probability and simulation episode evaluation. Simulation analysis of the proposed hierarchical MANET of 75 to 1000 nodes network with cryptographic primitives, protocols, and trust management reveals that ZRP routing protocol outperforms other routing protocols in terms of delivery ratio, delay, jitter and goodput.

Keywords*: MANET, RFID, wireless sensor networks, jitter and goodput.*

1. INTRODUCTION

Mobile Ad-hoc networks (MANETs) are a collection of autonomous terminals that communicate with one another by developing a multihop radio network and maintaining connectivity in a decentralised fashion. MANETs, and particularly wireless sensor networks (WSNs), are finding increasing applications in a variety of fields, including battlefield communication, emergency-relief personnel coordination, earthquake aftermath, natural disaster relief, wired homes, and also in today's highly mobile business environment, to name a few.
Nowadays, RFID frameworks are widely distributed. Its simplicity and speed make it a better choice than attractive tapes, bar codes, and smart cards for many applications. A complete RFID system includes tags, readers, and backend storage devices. A short-range wireless communication protocol is used these devices to identify themselves, be tracked, and keep track of data. Backend capacity frameworks have their own energy sources; tags receive this energy from the readers and use it to create reactions. Objects have tags attached to them so that their identification and other useful information can be stored. Information stored in the backend frameworks can be accessed by the reader, either to store it or to distribute it to other connected devices in order to increase its accessibility. There are four types of tags: active, inactive, semi-active, and semi-aloof tags that can be assigned. Uninvolved tags, on the other hand, do not have their own power source and must rely on the

electromagnetic waves emitted by readers to power their devices. Like dynamic tags, these low-memory and short-range devices can be used in a variety of ways and their information is stored once. As a result, the reader receives signals from the tags, which then reflect back to the reader, even though dynamic tags have an energy source and can send signals directly to the reader. Similarly to latent tags, semi-inactive tags are activated when a signal is received from the reader. Semi-inactive tags, in contrast to uninvolved tags, have an energy source that isn't used to elicit a response from the reader but is instead used to power an electronic circuit. When compared to dynamic tags, semi-detached tags operate at a slower rate, have a smaller battery, and have a shorter range of communication. Semi-dynamic tags may be dynamic or semi-inactive tags. In contrast to aloof or semi-latent tags, the power of semi-dynamic tags can be transmitted at greater distances. It is best to use these tags in noisy or obstructed environments.

For lower computing product management, a comparative analysis of three important management protocols for lower computing products is carried out in this chapter: Tan and Teo, Wen Lin-(WLH), Hwang's and Tseng's. It has been discovered that the protocol developed by Teo and Tan is a highly effective crucial management protocol for hierarchical networks. Toutefois, the protocol developed by Teo and Tan suffers from I exponential expansion of key emails as a result of powerful topology, (ii) energy loss as a result of the high proximity of nodes in a subgroup, (ii3) the absence of authentication, and (iv) vulnerable ahead secrecy. In part as a result of these flaws, particularly weaknesses (I) and (ii), the computational and correspondence price for lower-powered wireless and mobile devices is absurdly high. Specifically, this work extends Teo and Tan's circular hierarchical style to teams with a fixed number of participants, and it also makes Teo and Tan's protocol suitable for lower-powered wireless and mobile devices. It has been demonstrated that there is an increase of 6.6 percent of GEs for management that is critical when compared to Teo and Tan's protocol. Additionally, when compared to Teo and Tan's protocols, the proposed mechanism achieves significantly better results in terms of delay and throughput security, as well as delay in terms of authentication, confidentiality, and backward and forward secrecies.

2. REVIEW OF RELATED LITERATURE

Kumar, Agarrwal and Adarsh, Alok. (2020) An increasing number of innovative and resource-constrained products are recommending a variety of authentication schemes. The known security flaws in many of these systems preclude their use in real-world applications. For comparison, elliptic curve cryptography (ECC) based authentication mechanisms are recommended. The proposed authentication mechanisms are formally validated using automated little cryptographic primitives for useful resource constrained products. An evaluation on seventy-five, 150, and a thousand node networks found that the proposed protocol five provided the best overall performance in terms of least jitter and processing delay, as well as maximum throughput Protocol 5 has a minimum of 4.3 percent and a maximum of 61.9 percent improvement over other protocols when compared to other protocols.

Landaluce et al., (2020) RFID networks (Wireless sensors and rfid) and wireless sensor networks (WSN) are the foundations of the Internet of Things (IoT). RFID and WSN technologies work together to locate and monitor products, while collecting and disseminating data from interconnected sensors. Using RFID devices with identification features as sensing and computational platforms and as architectures of wirelessly attached sensing tags can be difficult in this context. This, along with the most recent advancements in WSNs and the integration of both technologies, has given rise to the possibility of new IoT applications. A review of these two technologies and the obstacles and challenges that must be overcome is provided in this paper. A few of these issues include energy harvesting efficiency, correspondence interference, fault tolerance, increased data processing capacity, price feasibility, and ideal element integration. IoT technology is also examined in terms of two emerging trends: the combination of WSNs and RFID in order to benefit from their complementary capabilities and the use of wearable sensors, which enable new promising IoT uses.

Al-Husainy et al., (2020) We're in the midst of the Internet of Things (IoT) era, where the uses of its like smart homes and smart cities collect very sensitive data gathered by IoT surveillance cameras and various other sensors or devices. Because these kinds of highly sensitive data must be transmitted across the IoT network to be prepared and saved on Cloud, security and privacy protection is critical. A light-weight encryption design has been proposed in this paper to meet the needs of IoT devices in terms of both mind and progress. Additionally, the encryption version provides an additional layer of protection for transmitted data by changing the encryption key on a regular basis. To make it even more difficult for an attacker, the proposed design uses a key size that's large enough to encrypt data. Experiment results show exceptional results, with an average of 170.7 ms of encryption time for an eighty-bit critical colour and an average PSNR of 7.7 when compared to other algorithms.

Bhushan, Sahoo and Bharat, Gadadhar. (2019) Many routing protocol requirements must be met as a result of WSNs' powerful topology, resource constraints, and distributed dynamics. Wireless sensor networks are made up of a large number of spatially distributed, low power, low cost, and smart autonomous sensors linked to one or more base stations that cooperatively monitor physical conditions or the environment such as stress, temperature, motion, or sound. The efficiency of any routing protocol is governed by two primary elements: network lifetime and energy conservation. Another difficult problem in WSNs is QoS support, and as a result, QoS conscious routing protocols have received a lot of attention in the last few years. In this document, we will first discuss a number of difficult elements as well as problems that affect the routing protocol layout of WSNs. In this paper, we classify different routing protocols in WSNs into three major groups: flat network routing protocols, hierarchical network routing protocols, and QoS conscious routing protocols. The report investigates flat network routing protocols such as reactive, proactive, and hierarchical networks, as well as hybrid protocol routing protocols such as chain-based, grid-based, area-based, and tree-based protocols. The post also goes over the various QoS types of routing protocols used in WSNs. Finally, we identified some open issues regarding the layout of routing protocols in WSNs.

Zemrane et al., (2019) Communication networks have seen significant advancement since their inception, progressing from wired networks to wireless communication networks with infrastructure, and now we are talking about wireless communication networks with no infrastructure, also known as MANETs, which are also known as mesh networks. Wireless communication networks, which do not require any infrastructure, allow for quick, efficient, and simple network deployment. They are frequently used in rescue operations following a natural disaster, to change the current network infrastructure, and even in the military environment. We concentrate our efforts in our work on the smart transportation system, which is superior to the conventional transportation system in terms of reducing the risk of human error in order to save lives, as well as the effective management of traffic congestion in order to save time and reduce energy consumption. There are numerous routing protocols available in MANETs; in this document, we compare the overall performance of several of these routing protocols when utilising various correspondence apps that are based on the HTTP, Voice, and FTP protocols.

Garaaghaji, Alfi and Ali, Alireza. (2019) When it comes to the technical definition, it is actually a collection of distributed nodes that are dispersed throughout a relatively small area and connected by wireless connections. Hierarchical algorithms divide a network into two levels of hierarchy based on the paths that are available to be taken through the network. The primary goal of this particular paper is to develop the best possible allocation algorithm for wireless networks by employing a fuzzy logic (FL) algorithm, specifically a fuzzy hierarchical algorithm, in order to maximise throughput while minimising latency. In order to increase system speed by decreasing the amount of information exchanged, FL is implemented because of the simplicity of its calculation. As a result of the findings, the proposed algorithm is demonstrated to be feasible.

Bruzgiene et al., (2017) In today's technological world, a variety of physical objects can be used to aid in the performance of a human task. In order to connect physical objects with the digital world, the web of Things is employed, a revolutionary engineering and a great answer that utilises heterogeneous networks and communication technologies to do so. Wireless sensor networks (WSNs) and mobile ad hoc networks (MANETs) interact with the Internet of Things in sensible environments, making it more appealing to customers and more profitable from an economic standpoint. It is possible to create new MANET IoT devices and IT-based networks by integrating wireless sensor and mobile ad hoc networks with the web of things. This ca allows for greater user mobility while also lowering network deployment costs. As a result, it raises new challenges for the network's various components. In this paper, the authors propose a routing option for the web of things system that combines WSN and MANET protocols. An effective strategy for reducing energy consumption in the global MANET IoT system is presented by the solution's investigation results And that's a step in the right direction toward a worldwide Future Internet infrastructure that can be relied upon.

3. PROPOSED METHODOLOGY

A hierarchical MANET is built with the integration of RFID Sensor incorporated products. This hierarchical network is made up of organisations. Every team has a subgroup controller and several subgroup members. This procedure for constructing a hierarchical MANET is expanded to provide routing as well as network security with improved performance. As shown in figure 1, a virtual node-based protected hierarchical network is built with the help of an authentication process and trust control.

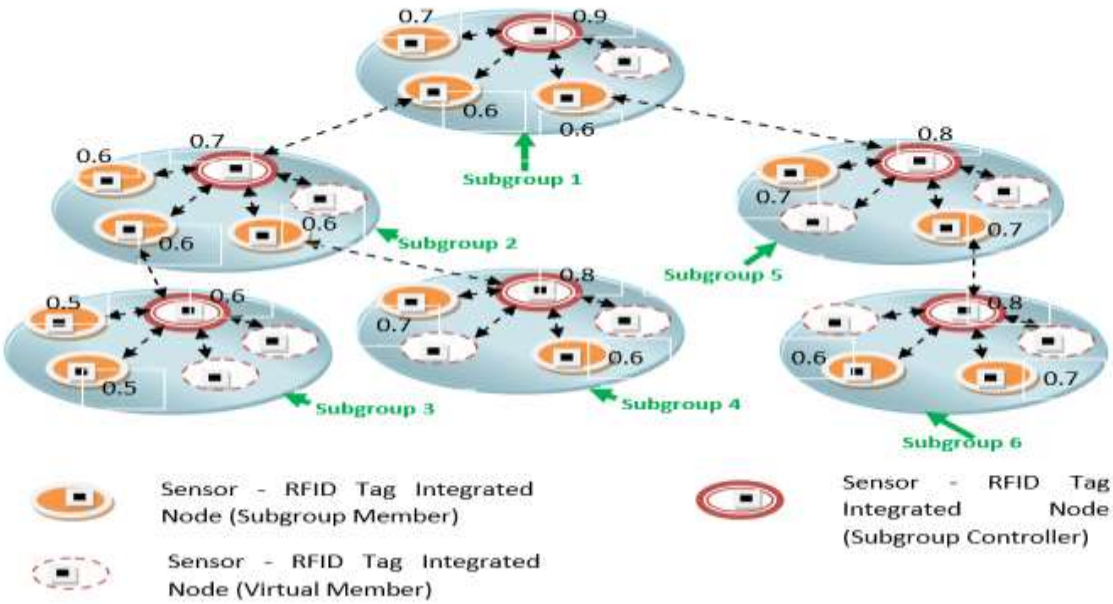

Fig 1: Constitution of virtual nodes based single-hop hierarchical network

Integration of authentication, distance bounding, and tag ownership transfer protocol present routing security at this point. The incorporation of trust control provides network security. The following are the steps taken to create a virtual node-based protected hierarchical MANET.

1. To begin with, it was assumed that all nodes were trustworthy.
2. A unique identifier is assigned to each node in the network.
3. Trust scores are generated by each node in the network. If a node's trust score falls below a certain value, it is not considered to be a part of the network. Figure1 depicts a trust score of less than 0.5 for each node in the hierarchy.
4. The original subgroup controller is considered to be the node with the highest trust score in the immediate vicinity. This subgroup controller is responsible for registering a new subgroup. This particular node, for example, has a trust rating of 0.9, which means that it has been assigned to a subgroup. Virtual nodes are added to subgroups if there are not enough real nodes in a given subgroup, so that the total number of nodes in each subgroup can be fixed. To put it another way, virtual nodes don't actually exist; they're programmable nodes that are added to the network in order to improve its performance. In hierarchical design, for example, each subgroup is actually running a total of five nodes. While some subgroups have 3 real and 2 virtual nodes, subgroups one and two each have 4 real and one virtual node.
5. To form subgroups at a higher hierarchical level, members of the original subgroup rub their nodes near you to authenticate. Until all nodes in a hierarchical network have been discussed, this particular procedure continues onward.
6. Subgroup controllers are chosen based on the highest trust score for each subgroup in a hierarchy of interconnected subgroups. Any member of a subgroup with a higher number of neighboring nodes is chosen to serve as the group's controller if two or more members of that subgroup have the exact same trust score. Subgroup controller is chosen arbitrarily when there are at least two or more subgroup members with similar trust scores and a similar number of neighbors.

3.1 Simulation Parameters

To see how these parameters were simulated, see Table 1. The ns 3 simulator was used to simulate a small to large network with packet sizes of 512 bits and data rates of 168 bits per second over an area of x thousand square metres.

Table 1: Simulation Parameters

Parameters	Value
Channel Type	WirelessChannel
Radio Propagation Model	TwoRayGround
Network Interface	WirelessPhy
MAC Type	802.11
Interface Queue	Priority Queue
Antenna	OmniAntenna
Max Packets in Queue	50
Protocols	AODV, DSDV, TORA, DSR, ZRP
X dimension of the topography	1000 meters
Y dimension of the topography	1000 meters
Mobility Model	Random Way Point Mobility
Data Rates	5 packets/second
Packet Size	512 bits
Simulator	ns-3
Simulation Time	1000sec

3.2 Packet Delivery

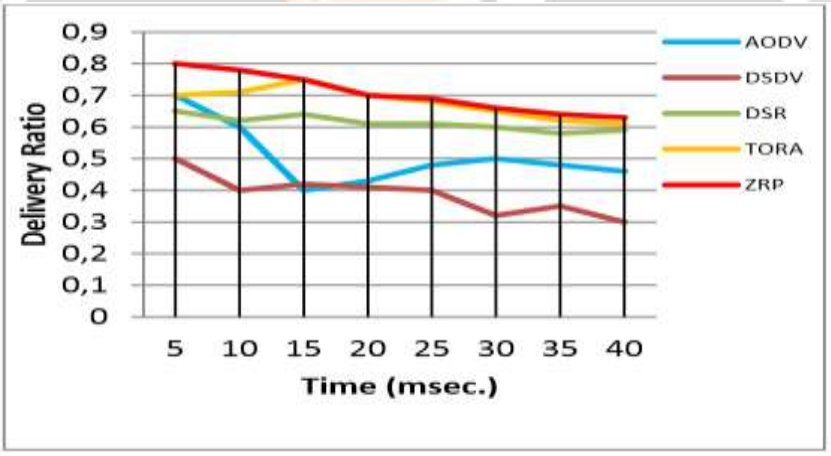

Fig 2: Delivery ratio for 75 nodes over MANET's routing protocols for 5 packets/second

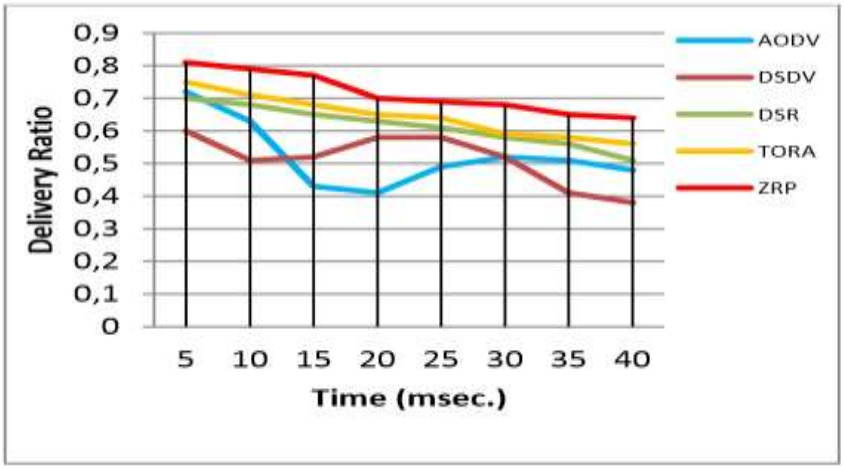

Fig 3: Delivery ratio for 150 nodes over MANET's routing protocols for 5 packets/second

3.3 Goodput

Non-overlapping phrases with high delivery ratios are actually a good idea. It's the total amount of useful information bits that a network sends to its endpoints in a given period of time. These three graphs clearly show the goodput for 75 nodes at extended tonnes of 0.1 packet/second, one packet/second and five packet/second (Fig. 4, 6 and 8), respectively. In terms of effective packet transmission selection, the ZRP protocol consistently outperforms the competition. In these scenarios, TORA and DSR have the worst overall performance. This is due to the fact that protocols use routing. It has also been discovered that data transmission improves as the number of packets delivered per second increases. Since the number of nodes available for interaction is sufficient even at lower packet fees, the network's congestion decreases as the number of nodes increases. Extendable tonne rates of 0.01 packet/second, one packet/second, and five packet/second are clearly shown in Figures 5, 6, and 7. Goodput is higher in 150-node scenarios than in 75-node scenarios because 75 more nodes are available to assist in handling the increased number of packets. ZRP protocol outperforms any other process in 150-node scenarios. The ZRP protocol's ability to function at a data rate of 0.1 packets per second is typical, and it's increasing exponentially as time goes on. ZRP has better throughput than 0.1 packet/second at data rates of one packet/second and five packets/second for 150 nodes. Other protocols' performance also rises in these scenarios, but by a smaller margin than the ZRP process. Additional findings show that in 150 node scenarios, ZRP's throughput progress is more or less straight line, whereas other protocols are less or less straight line.

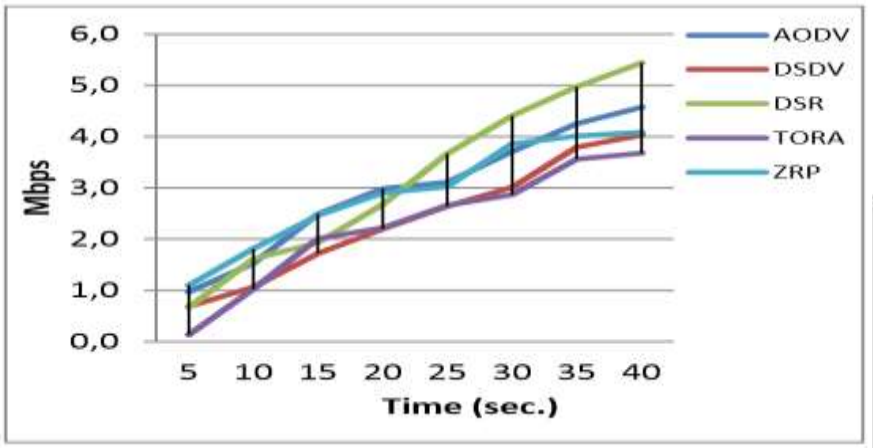

Figure 4: Goodput for 75 nodes for 0.1packet/second

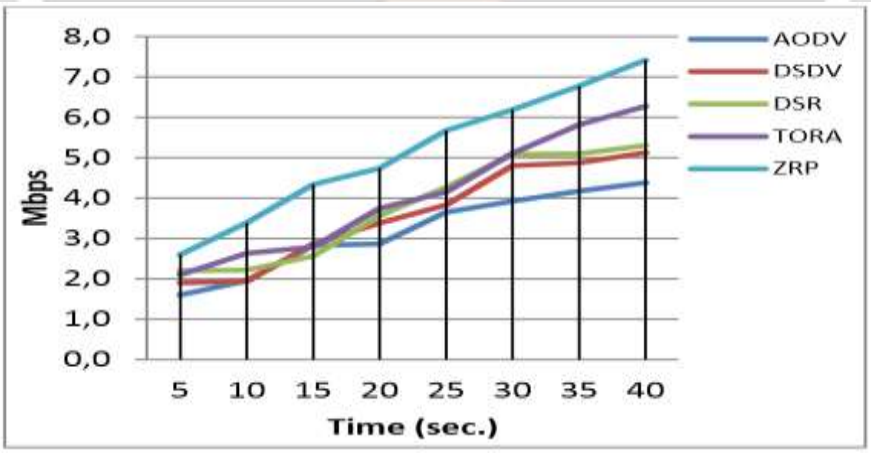

Figure 5: Goodput for 150 nodes for 0.1 packet/second

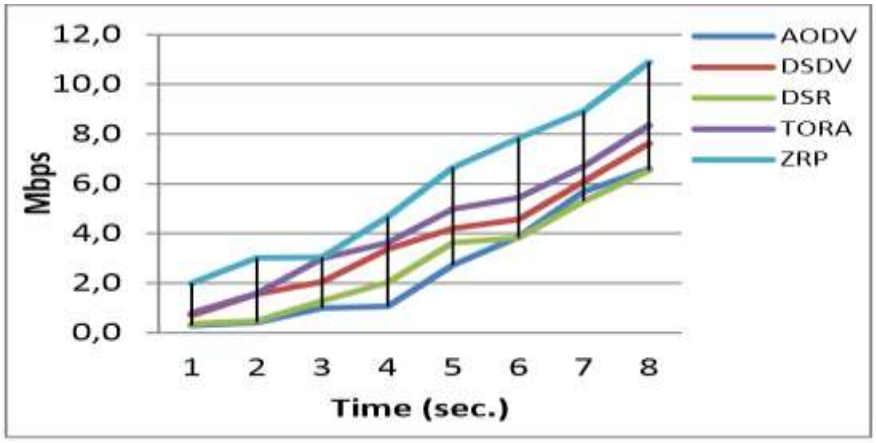

Figure 6: Goodput for 75 nodes for 1 packet/second

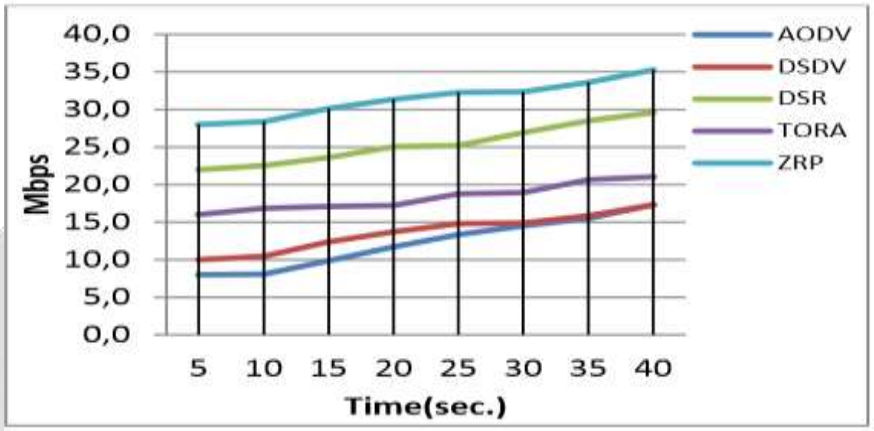

Figure 7: Goodput for 150 nodes for 1 packet/second

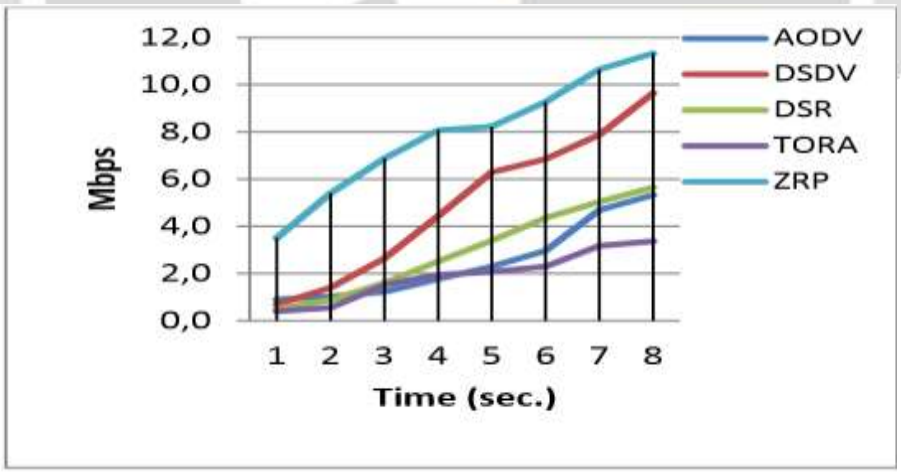

Figure 8: Goodput for 75 nodes for 5 packets/second

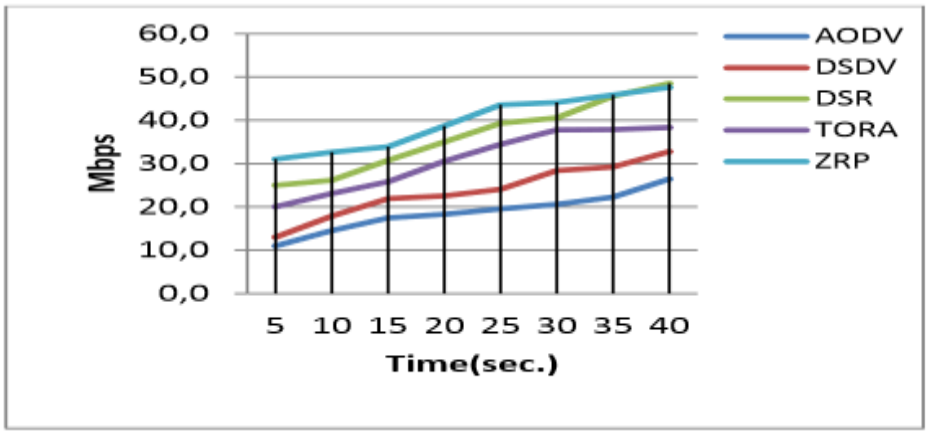

Figure 9: Goodput for 150 nodes for 5 packet/second

3.4 Jitter

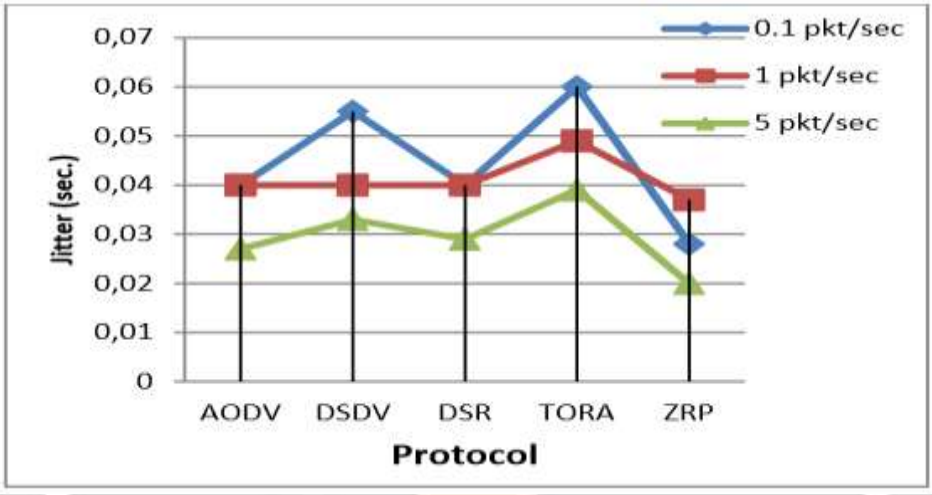

Figure 10: Jitter for 75 nodes at different delivery rate

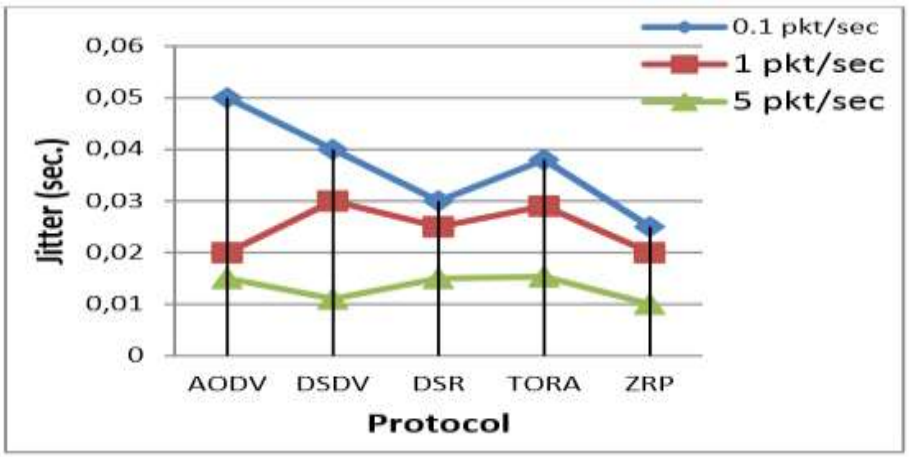

Figure 11: Jitter for 150 nodes at different delivery rate

In order to circumvent authentication on data packets that are vulnerable to collisions, a message digest attacker is built. Passive or active, this attacker intercepts data packets in order to learn the source and destination addresses. Predicate used to apply digest attacker is shown in Fig. 12 As the number of attacker nodes increases from zero to eight per subgroup in a 1,000-node hierarchical network, the postponed analysis of consensus establishment is shown in Fig. 5.29. Consensus establishment in a hierarchical network with an increasing number of attacker nodes is shown in Fig. 5.30. Authentication from a subgroup controller is required for an attacker node to join a subgroup, which makes it difficult for the nodes to reach consensus. As a result, the results show that the typical delay for establishing consensus is much greater when attackers are contained in subgroups than when they are present in a network. However, attackers are unable to communicate with nodes

due to their lack of authenticity in the next scenario. The subgroup controller can be overloaded by these unauthentic nodes, causing authentication delays. Compared to a delay due to the presence of a subgroup of attackers, this delay is comparatively short.

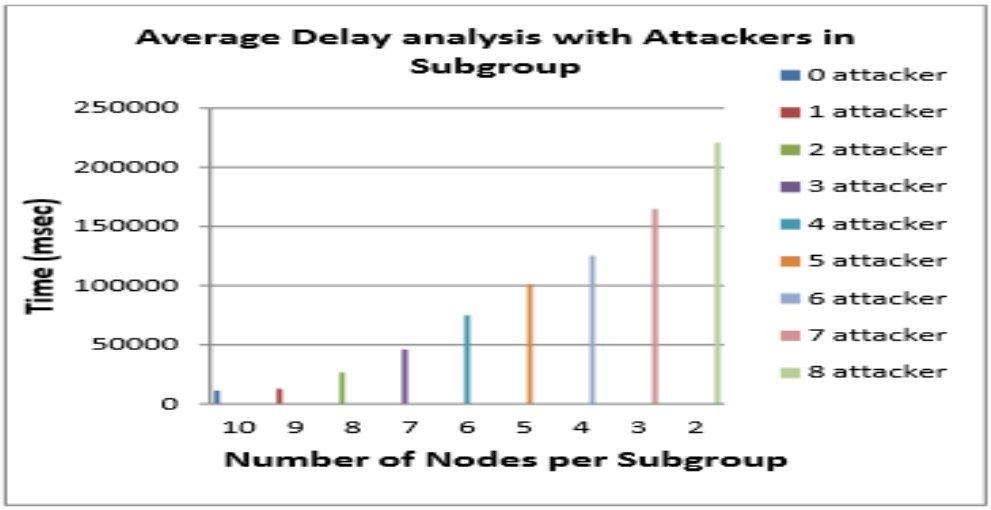

Figure 12: Delay analysis of a subgroup in presence of digest attacker

4. CONCLUSION

Every passing year will see an increase in the demand for RFID-Sensor integrated technologies in applications such as supply chain management, human services, anti-burglary devices, question tracking and tallying, get to control, and so forth. In both RFID and sensor networks, the network is under control. The integration of conventional cryptographic primitives and protocols will necessitate the use of infeasible resources from these devices, necessitating the advancement of technology.

Author provides a comparative analysis of three lightweight critical management protocols: Teo 186, Tan, Tseng, and Wen-Lin-Hwang, and in the second section, they provides a comparative analysis of three lightweight critical management protocols: Teo 186 and Tan, Tseng, and Wen-Lin-Hwang. It has been recommended that the Tan and Teo protocol be expanded. In connection with the proposed extension variants of key management, it has been discovered that the proposed protocols can be used to create and distribute keys in restricted networks with improved performance in terms of delay and throughput, as well as security in terms of authentication, confidentiality, and backward and forward secrecies.

In virtual nodes-based RFID Sensor integrated hierarchical MANETs, it was found that a lightweight and secure strategy of light cryptographic primitives as well as protocols outperformed all others. When compared to error-correcting fast, slow, and codes stage authentication or possibly different strike-protected schemes, the suggested pattern provides higher security at a lower cost. The degree of security against authentication attacks, as well as against distance bounding, ad hoc correspondence, and ownership transfer protocols, is investigated.

Simulations and modelling analyses of the proposed protocol have been carried out for networks ranging in size from small (seventy-five nodes) to large (hundreds of nodes). It has been discovered that networks using the suggested security protocols in conjunction with the ZRP routing protocol outperform the AODV, TORA, SR, and DSDV routing protocols in terms of jitter, delay, the presence of idle nodes, goodput, and energy consumption, respectively. It is necessary to conduct a modelling examination in order to detect hits in the presence of virtual, genuine, and attacker nodes in the network. It has been discovered that an increase in virtual nodes, or possibly attacker nodes, has increased the delay in consensus establishment because both cause overhead on the subgroup controller in a group of nodes to establish consensus.

5. FUTURE SCOPE OF THE RESEARCH

If we look at future RFID-Sensor integrated networks in comparison to RFID networks or wireless sensor networks, they will have better receiving wire plans, cloud capabilities and large memory limits, as well as a greater perusing and cross examination range, faster handling, and so on. The integration of ultra-lightweight cryptography with restricted operations can help to keep costs down while simultaneously improving security. With the probabilistic approach presented in this proposal for an improvement in the level of security in authentication and separation bouncing protocols, it can serve as a starting point for future investigations into identification, assemblage authentication and encryption, and secure ownership transfer protocols, which are required by the rapidly developing field of interest in lightweight cryptography.

6. REFERENCES

[1] Kumar, Adarsh &Agarrwal, Alok. (2020). An Efficient Outlier Detection Mechanism for RFID-Sensor Integrated MANET. 10.1007/978-3-030-16657-1_80.

[2] Kumar, Adarsh &Agarrwal, Alok. (2020). Comparative Analysis of Elliptic Curve Cryptography Based Lightweight Authentication Protocols for RFID-Sensor Integrated MANETs. 10.1007/978-3-030-16657-1_87.

[3] Kumar, Adarsh & Gopal, Krishna &Agarrwal, Alok. (2013). Outlier Detection and Treatment for Lightweight Mobile Ad Hoc Networks. 115. 750-763. 10.1007/978-3-642-37949-9_65.

[4] Kumar, Adarsh & Gopal, Krishna &Agarrwal, Alok. (2015). Novel trusted hierarchy construction for RFID sensor-based MANETs using ECCs. ETRI Journal. 37. 186-196. 10.4218/etrij.15.0114.0177.

[5] Kumar, Adarsh & Gopal, Krishna &Agarrwal, Alok. (2016). Design and analysis of lightweight trust mechanism for secret data using lightweight cryptographic primitives in MANETs. 18. 1-18.

[6] Kumar, Adarsh & Gopal, Krishna &Agarrwal, Alok. (2017). A novel lightweight key management scheme for RFID-sensor integrated hierarchical MANET based on internet of things. International Journal of Advanced Intelligence Paradigms. 9. 220. 10.1504/IJAIP.2017.082981.

[7] Landaluce, Hugo; Arjona, Laura; Perallos, Asier; Falcone, Francisco; Angulo, Ignacio; Muralter, Florian. 2020. "A Review of IoT Sensing Applications and Challenges Using RFID and Wireless Sensor Networks" *Sensors* 20, no. 9: 2495. https://doi.org/10.3390/s20092495

[8] Lee, Eric. (2011). Security in Wireless Ad Hoc Networks. Science Academy Publisher Science Academy Transactions on Computer and Communication Networks Copyright © Science Academy Publisher. 1.

[9] Liu H., Bolic M., Nayak A., and Stojmenovie I., "Integration of RFID and wireless sensor networks", Sense ID 2007 Workshop at ACN SenSys , Sydney, Australia, pp. 6–9, November 2007.

[10] Malla, Bala. (2016). Security and Trust Management for the Internet of Things: An Rfid and Sensor Network Perspective. 10.1002/9781119193784.ch4.

[11] Manifavas C., Hatzivasilis G., Fysarakis K., and Rantos K., "Lightweight Cryptography for Embedded Systems - A Comparative Analysis", 8th International Workshop, DPM 2013, and 6th International Workshop, SETOP 2013, Egham, UK, pp 333-349, September 12-13, 2013.

[12] Manjulata, A.K.. (2014). Survey on lightweight primitives and protocols for RFID in wireless sensor networks. International Journal of Communication Networks and Information Security. 6. 29-43.

[13] Miller L. E., "Indoor Navigation for First Responder: A Feasibility Study", Technical Report, National Institute of Standards and Technology, Advanced Network Technologies, Feburary 2006.

[14] Mitsugi J., Inaba T., Patkai B., Theodorou L., Sung J., Sanchez Lopez T., Kim D., McFarlane D., Hada H., Kawakita Y., Osaka K. and Nakamura O., "Architecture development for sensor integration in the EPCglobal network", Auto-ID Labs White Paper, White Paper Series, 2007.

[15] Mtibaa, A. and Harras, K. A. "FOG: Fairness in Mobile Opportunistic Networking", 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), DOI: 10.1109/SAHCN.2011.5984906, pp. 260–268, 201

[16] Mujahid U., Najam ul islam M., and Ahmed J., "Ultralightweight cryptography for passive RFID systems", Cryptology ePrint Archive: Report 2013/847, version 20131231:132512, December 2013.

[17] Mukherjee, Sankar & Biswas, G.P.. (2017). Networking for IoT and applications using existing communication technology. Egyptian Informatics Journal. 19. 10.1016/j.eij.2017.11.002.

[18] Nezhad, Alireza & Miri, Ali &Makrakis, Dimitrios. (2008). Location privacy and anonymity preserving routing for wireless sensor networks. Computer Networks. 52. 3433-3452. 10.1016/j.comnet.2008.09.005.

[19] K. Fishkin and J. Lundell,"RFID in healthcare,"inRFID: Applications,Security, and Privacy, S. Garfinkel and B. Rosenberg, Eds. Reading,MA: Addison-Wesley, 2005, pp. 211–228.

[20] K. P. Fishkin, S. Roy, and B. Jiang,"Some methods for privacy in RFIDcommunication,"inProc. 1st Eur. Workshop on Security in Ad-Hoc andSensor Networks, 2004.

[21] Keng Seng NG, Winston K.G.SEAH, "Routing security and Data Confidentiality for Mobile Adhoc Networks", Proceedings of the 5thIEEE conference on Mobile and Wireless Communication Networks, pp 821-25

[22] Khan, Khaleel & U Zaman, Rafi & Reddy, A. & Hafeez, Kashifa & Sultana, Tabassum. (2008). A hierarchical approach of integrating Mobile ad hoc Network and the internet. 1-4. 10.1109/ICON.2008.4772646.

[23] Kuiper, E. and Nadjm-Tehrani, S. "Geographical Routing With Location Service in Intermittently Connected MANETs", IEEE Transactions on Vehicular Technology, Vol. 60 , No. 2, pp. 592-604, 2011.