PERFORMANCE ANALYSIS OF UHF, RFID SECURITY & ENERGY EFFICIENCY USING NS2

Priyadarshini A Dass[1], Dr. B. Sivakumar[2]

[1]M. Tech Student, Department of Telecommunication Engineering

[2]Professor, Department of Telecommunication Engineering

[1,2]Dr. Ambedkar Institute of Technology, Bengaluru

Abstract: RFID [Radio Frequency Identification Devices] systems have picked up prominence in recent times where these systems are deployed in large scale in commercial application and enterprise areas. Since the cost is low, systems can be implemented in supply chain management and these systems replaces barcode devices in near future RFID systems poses a number of research challenges such as interfering mitigation, data quantity optimization and security over RF media [1]. Many new measures are performed to eliminate this issues are been considering but due to highly combined nature. In the proposed work a future security of improved protocol with physical authentication and information cryptographic mechanism between secure source and destination for the UHF, RFID system is implemented in the simulation platform where it is exposed to several scenarios, and upcoming standards the topic includes authentication, access control, fault response, encryption decryption, dynamic privacy protection, hardware implementation algorithm, case study and applications [2]. The implementation also performs the comparison of the performance metrics of three protocols of wireless network that is RFID-Radio Frequency Identification Device Protocol, AODV- Ad-hoc On Demand Vector Routing Protocol and DSR-Dynamic Source Routing [3]. The performance metrics used for evaluation are as average energy consumption, delivery ratio of packets, overall throughput efficiency, and bit error rate. Simulation result shows that RFID Protocol has considerably high performance. The implementation simulation is done by using NS-2.35 Network Simulator.

Index Terms- RFID, RFID Protocol, AODV, DSR, Data Security, Neighboring Nodes, Parameters, Performance Analysis, Energy Efficiency

INTRODUCTION

RFID systems are highlighted as, an upcoming technology for spontaneous identification. Though, different barcodes these tags can be scanned in longer range, exposing them to unauthorized scanning by spiteful readers and to various attacks, including duplicating attacks [4]. Hence a secured protocol for RFID systems are required to guarantee the secrecy and authentication between each RFID systems. RFID systems poses a number of research challenges such as interfering mitigation, data quantity optimization and security over RF media. Many new measures are performed to eliminate this issues are been considering but due to highly combined nature of, RFID Systems is a problem to evaluate them in real fault environment.

In the previous work Rahma et al., [1] states that the negligible effort and low operation intensity of UHF RFID tags, interchanges between tags and per users are not dominant. Enhancement in security and comfort of UHF RFID structures where assessing the framework energy and security of used agreements, approach will authorize to suggest improvement of innovative, other reliable and safe protocols. Bilal et al., [2] another basic confirmation tradition recalling the prerequisites and making usage of the present exercises without development of any exorbitant one the proposed tradition shows that it is impenetrable to each one of the ambushes possible in case of Gossamer tradition. Namrata et al., [3] insights the distant invention is option active fame step by step. Execution of conventions for three remote systems: DSDV, AODV and DSR. Execution measurements utilized aimed at development remain normal vitality utilization, bundle conveyance proportion, jitter, throughput, Remaining Energy, Total Delay. Replica results demonstration that, the AODV has significant best execution over any number of hubs. Abdelmalek et al., [5] exhibits, EPC Class 1 GEN2 tag are ease labels which are at times utilized for basic or secure applications. Expanding their strength isn't unimportant because of the extensive variety of mistake sinks. Additionally expanding the power must minimally affect the pass on region yet additionally should fit with an institutionalized convention. Fritz et al., [6] another on-line testing method empowering area by names deformations to redesign system steadfastness and availability. Next System C models RFID structure is planned method to deal with calculate test game plans. As the response for enhance system steadfast quality is presented. Arini et al., [7]the extended ns-2 outline work to incorporate help for RFID frameworks, and represents their utility with an execution of Localized Probabilistic Algorithm (LPA) utilized for stack adjusting in RFID framework.

PROBLEM FORMULATION

Motivation and necessity is to design and provide an effective and reliable solution that addresses the security problem and energy efficiency in RFID Devices. The solution ensures effective means of identifying attacks, recovering falsely accused nodes and provides a secure path for communication among the nodes in RFID Device. A future security improved protocol with physical authentication and information cryptographic mechanism between secure source and destination for the UHF, RFID system is implemented in the simulation platform where it is exposed to several scenarios, and upcoming standards the topic includes authentication, access control, fault response, encryption decryption, dynamic privacy protection, hardware implementation algorithm, case study and applications.

PROPOSED SYSTEM

The proposed system includes five phases and implementation flow chart is as shown below in the Fig: 1 implementation flow chart:

- Initializing network
- Selecting source and destination
- Securing data
- Finding true response
- Packet transmission
- Protocol comparison

1. INITIALIZING NETWORK

In this stage the creation of nodes takes place by providing labels to identifiy each node and deployment of nodes in dynamic manner to check nodes active state sample packet transmission is done. Overlapping nodes moved to random postion in order to get minimum distance and sample packet transmission is done to check active state of node to the moved location.

2. SELECTING SOURCE AND DESTINATION

User selects source and destination, and if they are found to be neighbors using distance formula then a message is generated stating that they are neighbors. Re-selection of source and destination is performed.

3. SECURING DATA

In this stage securing the data is achieved by encrypting and decrypting data. Hardy algorithm is used for securing data where user provides key ‘E’ to encrypt at sender side and key ‘D’ to decrypt at receiver end. Therefore third party cannot access the data anywhere in the network since data is in crypt form. In the absolute path securing process can be viewed. In the proposed work, message.txt (absolute path) indicates original message, message_crypt.txt(absolute path) indicates encrypted message. message_crypt_decrypt.txt (absolute path) indicates decrypted, message.neigh1.txt shows the list of neighboring nodes of source and destination.

4. FINDING TRUE RESPONSE AND PACKET TRANSMISSION

Here the data is transmitted via intermediate nodes called to neighboring nodes. If the neighbor’s response is found to be fake using specified response time, then the packets are dropped. Sender waits for a specified time instant then the packets are transmitted to destination.

5. PROTOCOL COMPARISION

The received data is analyzed for three protocols that are AODV, DSR, and RFID.

AODV

Adhoc-On DemandVector routing protocol is a reactive routing protocol which is related to source and destination number to avoid infinity count and loop backs this may occur at process of routing tabulation. If a node wants to transmit data then it sends a route request message in order to get a routing service [RREQ]. The routing table maintains all the information related to routing operation and a node can transmit data from source to destination using the routing table without over heads or over-lapping [5].The protocol works on two functions namely route discovery and route maintenance. In route discovery the routes are discovered using the updated routing table and the discovered routes are monitored until they are required by the initiator node.

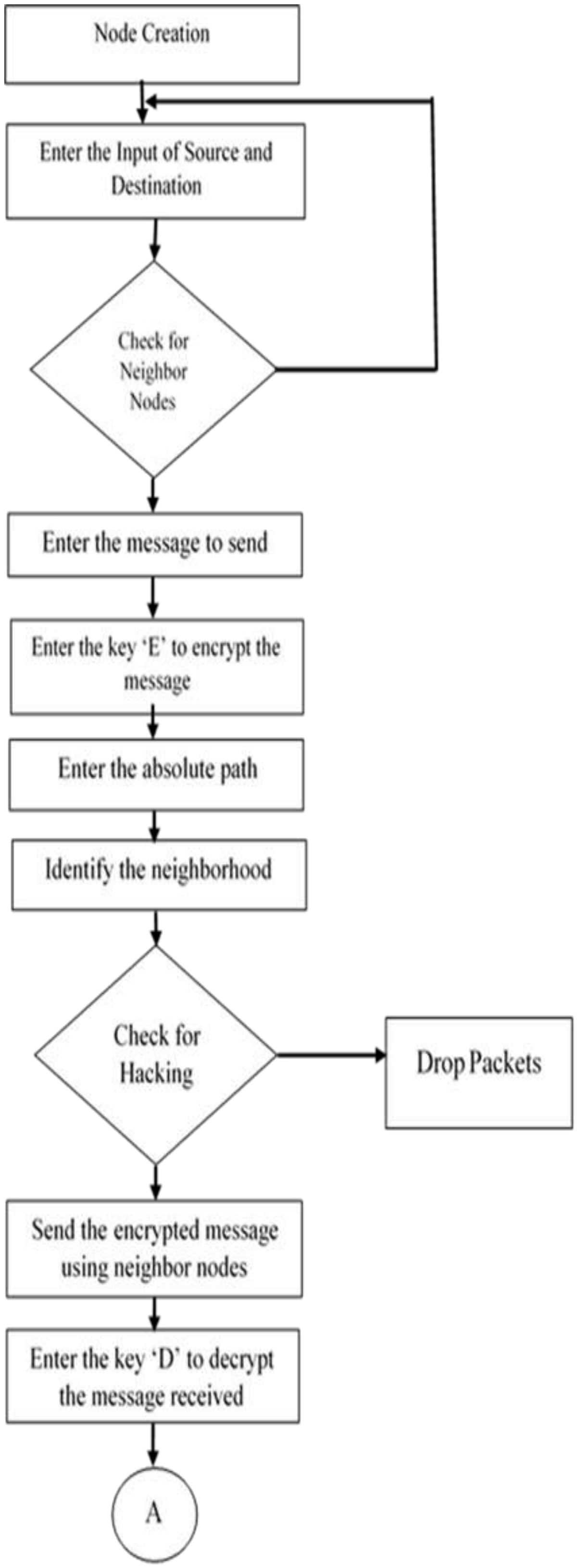
DSR

Dynamic Source Routing is a basic re-active protocol which uses two functions namely discovering of routes and maintaining of routes, these are implemented on ad-hoc network, in the absence of routing table control messages are used. The main operation of routing source is where the nodes are placed with packet headers with route which maps from source to destination. Every node in the network saves its address of the recent process, discovered nodes by overflowing in neighbor node transmission, when identification of route fails this process is initiated which achieves high transmission rate and loop free operation. This process provides service for Uni-direction and Multi-direction. It also provides communication to wireless devices in multiple network interface .hence it plays vital role in tactical communication since nodes in military tasking has different signal ranges with different networks

RFID

Radio Frequency Identification Devices Protocol, RFID module1 was created on discharge NS-2.35 test system. Execution is made using C++. There session controls are indicated using standard likewise executed. Orders indicated, for example, WRITE, SELECT, READ, are not executed meanwhile which don't influence distinguishing proof processes execution [6]. With a specific end goal to mimic the ID procedure, the distinction from total standards as in figure standards where the messages traded toward forwarding an arbitrary cipher [called as RNG16] earlier, the tag forward the own identification. Unreceptive to crash strategies we have discarded this progression which does not influence the module exactness since this progression is not meant execution assessment. Radio frequency identification devices protocol is a hybrid protocol. Where the operation depends on the geographic location of node in network [7]. Therefore the information can be obtained using GPS devices into communication network .here every node must know its own location and its neighboring node location .hence every node in the network broadcasts its address in the co-ordinates by all neighboring node .then the data is transmitted using the decision made by the algorithm of source and destination here location-lookup-algorithm to map the node address in its location. Exchange of information using periodic routing table in order to locate the address of source and destination. Absence of table it uses re-active approach therefore RFID uses two routing algorithm to transmit data from source to destination the objective of the protocol approach is to minimize overheads and increase the ratio of packet delivery and monitor the network topology[8].

PROPOSED SYSTEM IMPLEMENTATION FLOW


Node Creation
Enter the Input of Source and Destination
Check for Neighbor Nodes
Enter the message to send
Enter the key 'E' to encrypt the message
Enter the absolute path
Identify the neighborhood
Check for Hacking
Drop Packets
Send the encrypted message using neighbor nodes
Enter the key 'D' to decrypt the message received
A

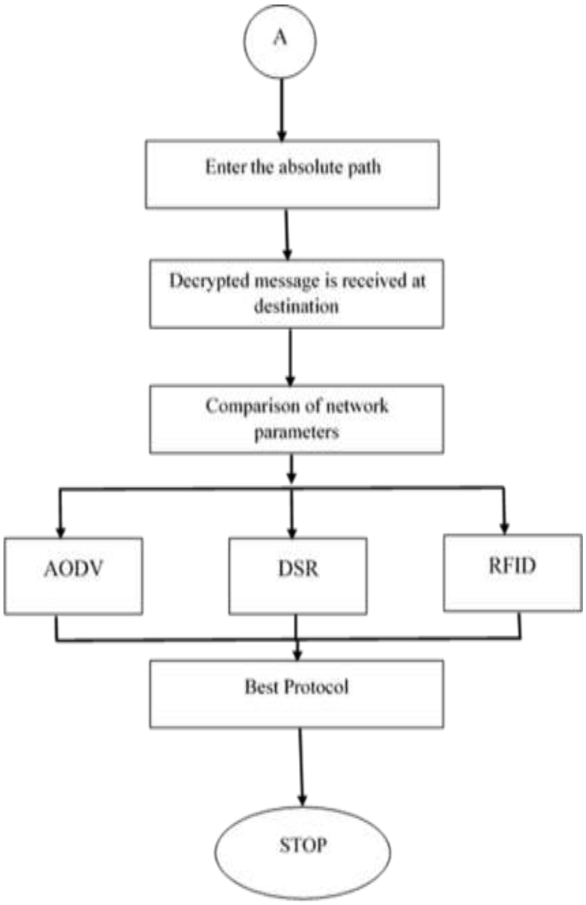
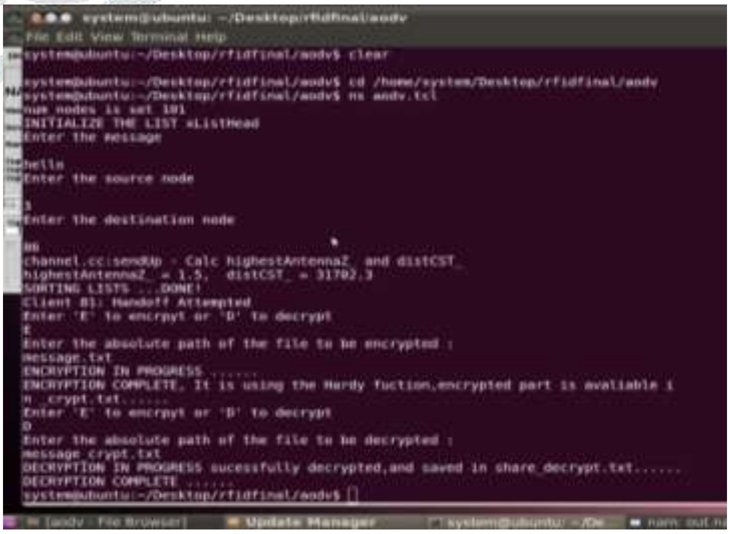

A
Enter the absolute path
Decrypted message is received at destination
Comparison of network parameters
AODV
DSR
RFID
Best Protocol
STOP

Fig 1: Implementation flow chart

RESULT AND DISCUSSION

In the output of proposed system is generated using NS 2.35. Output of NAM window is shown below. The fig 2, shows command window output shows selection of source and destination dynamically. If the selected source and destination are less than the minimum distance an error message appears in the command window stating that they are neighbors. The source and destination are to be reselected. To encrypt message 'E' key is entered and 'D' key to decrypt where this file can be viewed in the absolute path.


system@ubuntu: ~/Desktop/rfidfinal/aodv
File Edit View Terminal Help

```
system@ubuntu:~/Desktop/rfidfinal/aodv$ clear

system@ubuntu:~/Desktop/rfidfinal/aodv$ cd /home/system/Desktop/rfidfinal/aodv
system@ubuntu:~/Desktop/rfidfinal/aodv$ ns aodv.tcl
num nodes is set 101
INITIALIZE THE LIST xListHead
Enter the message

hello
Enter the source node

3
Enter the destination node

86
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 31702.3
SORTING LISTS ...DONE!
Client 81: Handoff Attempted
Enter 'E' to encrpyt or 'D' to decrypt
E
Enter the absolute path of the file to be encrypted :
message.txt
ENCRYPTION IN PROGRESS ......
ENCRYPTION COMPLETE. It is using the Hardy fuction,encrypted part is available i
n _crypt.txt......
Enter 'E' to encrpyt or 'D' to decrypt
D
Enter the absolute path of the file to be decrypted :
message crypt.txt
DECRYPTION IN PROGRESS sucessfully decrypted,and saved in share_decrypt.txt......
DECRYPTION COMPLETE ......
system@ubuntu:~/Desktop/rfidfinal/aodv$ 
```

Fig 2: Output on Command Window

Fig 3, shows the creation of nodes ,where the nodes are placed in random manner and in random distance, here node0- node 90 are created .Nodes are represented with label name 0-90 and in color green. Node configuration is observed where the color of nodes are changed from green to black in order to indicate processing has been started.Then sample packet transmission where the nodes from 0-90 are in active mode here boardcasting of sample packets can be observed.

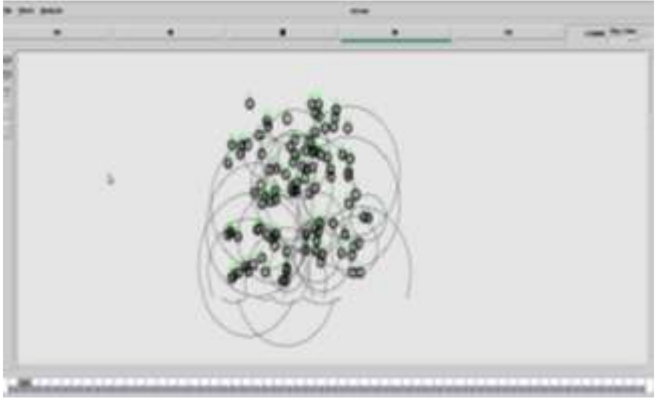


Fig 3: Node creation and Dyanmic Nodes Placement

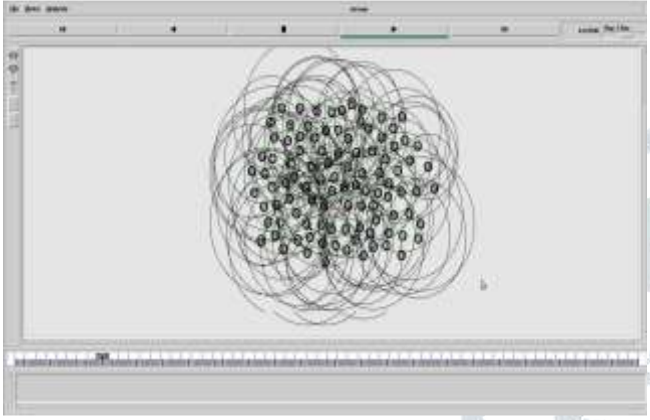


Fig 4: Broadcasting at Replaced Dynamic Location

The Fig 4, shows replacement of nodes in random position in order to eliminate overlap of nodes .Here nodes move randomly and acquire random position with minimum distance.Sample packet transmission is done to check active state of node to the moved location.

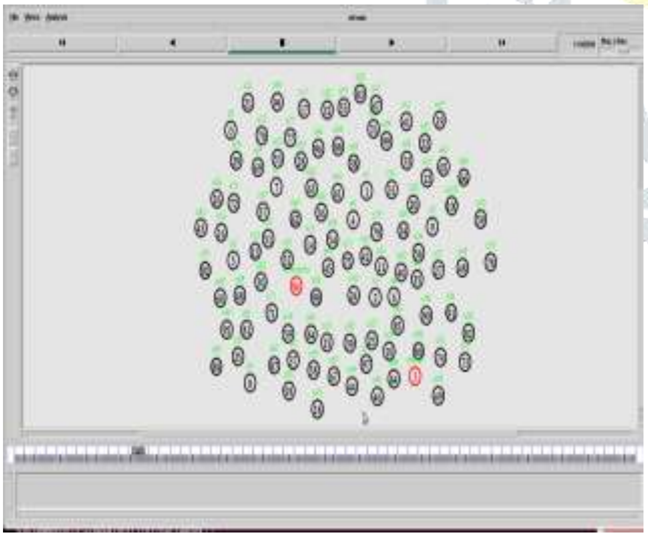


Fig 5: Selection of Source and Destination

The Fig 5, shows dynamic selection of source and destination node which are highlighted in red color.

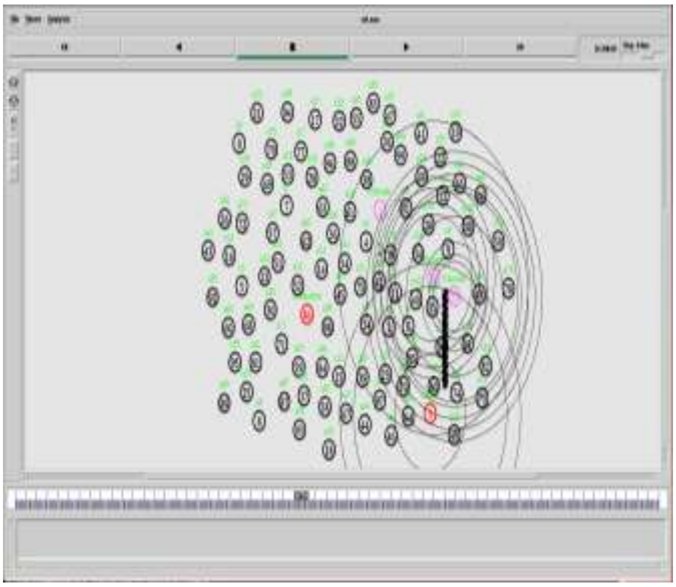


Fig 6: Packet Drop due to Fake Response

In Fig 6,nodes highlighted in purple color are neighboring nodes which help in transmission of packet from source to destination. The fake response of neighboring nodes causes packet loss as observed. Fake response can be identified using specified time instance. At this time hackers can only get crypted data. Sender waits for a specified time instant after which the packets are Re-transmitted using newly identified neighbors to destination as shown in the figure 7.

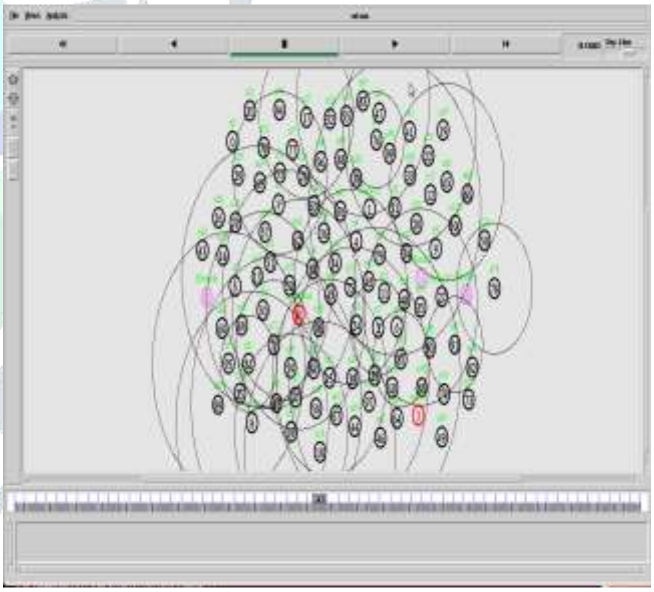


Fig 7: Data Transmitting from Source to Destination using Neighboring Nodes

The Fig 7, shows the data transmitting from source to destination using intermediate nodes called to neighboring nodes at the specified response time to transmit data.

The Fig 8, 9, 10, and 11 shows comparison graph of AODV, DSR, and RFID routing protocols. For the parameters Packet Delivery Ratio, Throughput, Residual Energy and Bit Error Rate respectively.

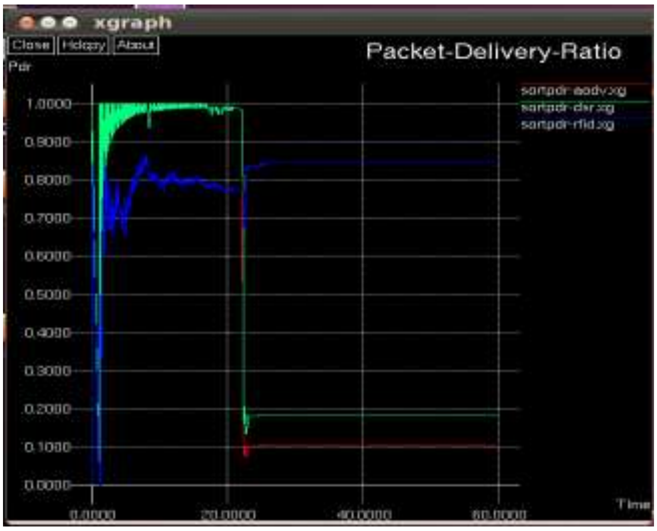


Fig 8: Comparsion graph of AODV, DSR, RFID,in terms of PDR

Table 1: Comparison table of AODV, DSR, and RFID in terms of PDR

Parameter PDR	Sent packets	Received packets
AODV	100126	324
DSR	100126	328
RFID	328	324

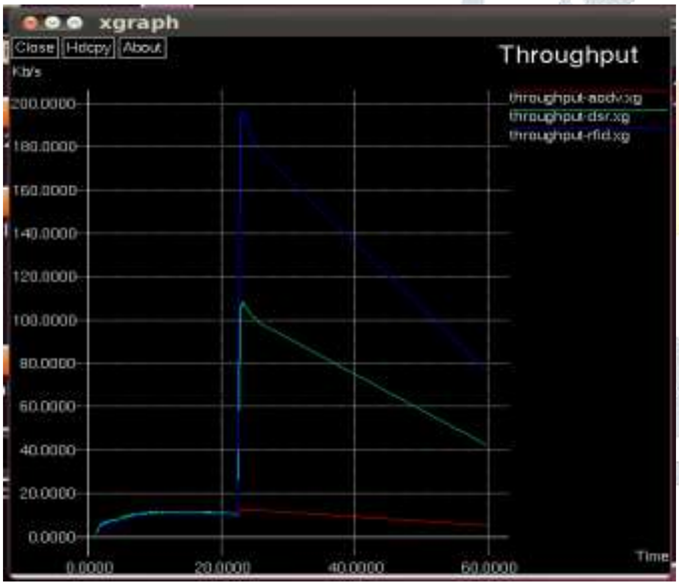


Fig 9: Comparsion graph of AODV, DSR, RFID,in terms of Throughput

Table 2: Comparison table of AODV, DSR, and RFID in terms of Throughput

Parameter Throughput	AODV	DSR	RFID
Sent packets	100126	100126	328
Received packets	324	301	324
Total no. packets	100450	100427	652
Throughput in percentage	32%	30%	98%

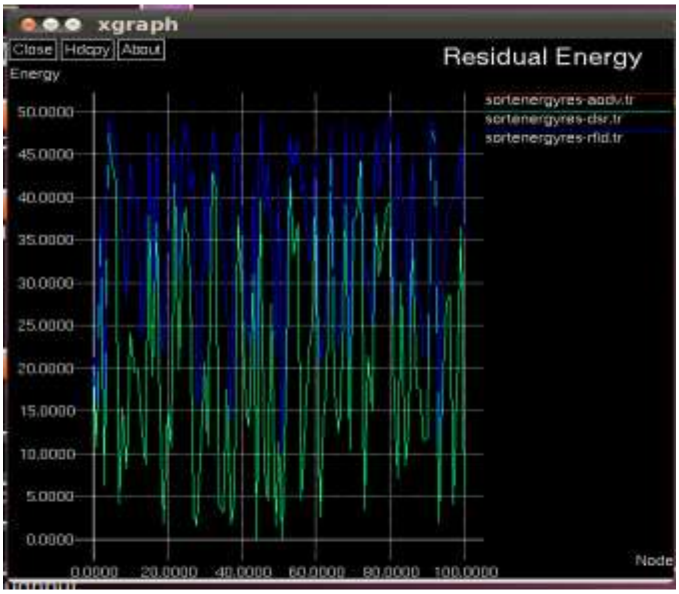


Fig 10: Comparison graph of AODV, DSR, RFID, in terms of Residual Energy

Table 3: Comparison table of AODV, DSR and RFID in terms of Residual Energy

Nodes	Residual energy in joules		
	AODV	DSR	RFID
0	19.20	19.20	41.20
20	15.10	15.10	46.11
40	27.67	27.6	49.31
60	40.31	40.31	45.20
80	39.37	39.37	49.31
100	5.07	5.07	47.08

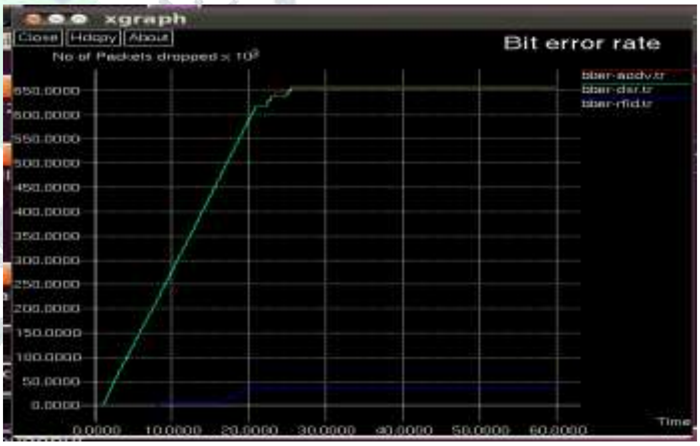


Fig 11: Comparison graph of AODV, DSR, RFID, in terms of Bit Error Rate

Table 4: Comparison table of AODV, DSR, and RFID in terms of Bit Error Rate

Parameter Bit error rate	No of bits lost in kbps
AODV	775934
DSR	127636
RFID	40133

Table 1,2,3,4 describes comparison analysis of the above graph, it is seen that performance of AODV is very low in terms of PDR, Throughput, Residual energy. Performance of DSR is better than AODV but less than RFID, that also describes performance of RFID is best compared to AODV and DSR as observed in the graph PDR, Throughput, Residual Energy is high compared to

AODV and DSR. Where lost bits rate is very less as compared to AODV and DSR.

Assessment of future research in the RFID Protocols, on request Routing calculation in remote sensor systems is an emerging research topic, since it has extraordinary research essentialness in better routing and prolonging network life cycle. For efficient use of available energy of sensor nodes can be implemented in various routing protocols. Evaluation of dedicated counter measure for robustness enhancement can be implemented against the fake response. Evaluation can be performed on other protocols based on authentication security issues and also evaluating simulation of fault environment. And can be performed on duplicating attacks over the system and rectifying the issues. Also compacting the various protocols with RFID device protocol to identify efficient algorithm to resolve various technical issues and also improving high speed data transmission with lower loss.

CONCLUSION

The implementation in this project is tended with the issue of limitation of energy required for genuine operation of remote sensor systems. The implemented work introduces the new method to secure data, by encrypting the sender data by key provided by the sender and decrypting the receiver data by key provided by the receiver, here this process can be viewed in the path specified by the user here it uses intermediate nodes known to be neighbor node to transmit data from source to destination, and hence the hacker cannot hack the data since the data is in crypt form. It also checks for the specified response time in order to know the fake response which response at the unspecified time. Here this process is implemented in different protocols such as AODV, DSR, and RFID. Here the process is evaluated with respect to different protocols in terms of evaluating metrics such as bit error rate, throughput, energy efficiency, packet delivery ratio. As observed in the simulation output, RFID (hybrid protocol) as the best performance with respect to securing the data, less consumption of energy, high packet delivery ratio, low bit error rate and high throughput efficiency when compared to AODV and DSR routing protocols.

REFERENCES

[1] AriniBalakrishnan, Swetha Krishnan “Simulation of RFID platform on NS-2”in Advanced Computer Networks ,3rd International Conference on IEEE,pp.23-34.December 2005.

[2] G. Fritz, V. Beroulle, M. D. Nguyen, D. H´ ly et al., “Rfid system on-line testing based on the evaluation of the tags read-error-rate”. IEEE Transactions On Automation Science and Engineering, Volume 6, NO. 1, JANUARY 2009.

[3]AbolfazlAkbari, Mehdi Soruri, “A New AODV Routing Protocol in Mobile Ad-hoc Networks”. World Applied Sciences Journal, ISSN 1818-4852, June2012.

[4]O. Abdelmalek, D. H´ely, and V. Beroulle, “Epc class 1 gen 2 uhf rfid tag emulator for robustness evaluation and improvement,” in Design & Technology of Integrated Systems in Nanoscale Era (DTIS), 8th International Conference on IEEE, pp. 20–24, 2013.

[5] Kiranpal Kaur, Naveen Kumari “An Approach to Enhance the Energy Efficiency of RFID Protocol using NTP Protocol” International Journal of Computer Science and Information Technologies, Vol. 5 (1) ,pp-724-727 ,August2014.

[6]Namrata S. Shinde, Dipit D. Shingade, Pranali D. Sonawane, “Performance Analysis of Energy Efficient AODV Routing Protocol Using NS 2.34” International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 4, Issue 4, pp. 10-15 ,April 2015.

[7]Z. Bilal, A. Masood, and F. Kausar, “Security analysis of ultra-lightweight cryptographic protocol for low-cost rfidtags: Gossamer protocol”. International Journal of Computer Applications (0975 – 8887) Volume 170 – No.1, July 2017.

[8]Rahma BEN FRAJ, Vincent BEROULLE, Nicolas FOURTY and Aref MEDDEB, “A Global Approach for the Improvement of UHF RFID Safety and Security’’ in, Design & Technology of Integrated Systems in Nanoscale Era(DTIS), 12th International Conference on IEEE, pp. 20-24, 2017

BIOGRAPHIES

Priyadarshini A Dass received the B E degree in Telecommunication Engineering from Dr. Ambedkar Institute of Technology, Bangalore and currently pursuing her Masters in Digital Communication and Networking in Dr. Ambedkar Institute of Technology, Bangalore. Her research interests include Communication Engineering, Wireless Sensor Networks and Digital Communication.

Dr. B. Sivakumar has obtained his BE (E & C), M.E (Applied Electronics), Ph.D. (Information & Communication Engineering) from Anna University. He has got rich teaching experience of 30 years and specialized in the area of wireless communications. He has published more than 150 National/International Journals & Conference. He has received 3 best paper awards in National/International Conferences. He has also filed a patent. He is in AICTE expert committee member and also participates in BOS/BOE of various autonomous Institution. He has produce 3 Doctoral scholars and presently guiding 5 doctoral scholar of VTU and PRIST University. He has delivered many expert lectures and keynote addresses in conference. He has obtained AICTE research grants to the tune of 30lakhs.