Improvising Reliability and Security in Multiple Relay Network using Optimal Scheduling

S.J. Subhashini, B. Stalin, J. Vairamuthu

Abstract: ***In the real-time scenario involving wireless sensor networks, the data forwarding and data gathering procedures are taking place from the remote environment. With the involvement of heterogeneous architecture and multi-hop data transmission paths, there lies a serious threat for secured data communication. There may be chances of data attacks either from the inside intruder or from the external intruder. The problem of data flow attack by adding malicious information, viz. Data injection attack and outside arbitrary attack, viz. Byzantine attacks are found to be more dangerous and cause vulnerability for the wireless sensor network. So improving the reliability and security in multi-relay networks is very much essential. In this work, the practical approach of detecting data injection and Byzantine attacks using the proposed method of random network coding is performed. Then, as improvisation measure, the priority scheduling algorithm is implemented to effectively schedule the data transfer. Real-time packets with highest priority in the distribution queue are placed first in the processing mechanism. The remaining packets are arranged based on the position of the sensor nodes and are placed in separate queues. Least priority packets can obstruct the dispensation of their direct higher precedence packets after waitlisted for a certain number of time frames. Simulation results using the NS2 environment show that using the priority scheduling algorithm has good performance values in terms of the packet delivery ratio, throughput and delay. Also, the attack detection metrics such as false positive ratio and detection ratio are also improved when using the priority scheduling algorithm. Thus an improvised priority algorithm for an uplink scheduler in WSN is implemented to increase the performance and detection metrics.***

Index Terms: Byzantine attack, Data injection attacks, Intruder attacks, Reliability, Scheduling, Security, Wireless sensor network.

I. INTRODUCTION

A wireless sensor network is formed by thousands of sensor nodes linked via wireless channel means in a single network path. The same is shown in Figure 1. Low power transceivers are deployed in the wireless sensor nodes in the WSN environment. Another significant feature of WSN is the self-organization of intra-network connectivity. Self-organization of the network allows randomly distributed sensor nodes and sinks to automatically form a WSN. In addition, when the network is in use and there are connection issues with some sensor nodes, it doesn't cause the whole system to fail. In such case, WSN simply shifts its mode of operation in order to not use the lost nodes for data transmission. This characteristic of WSNs noticeably simplifies their installation and maintenance, and also makes creating WSNs with millions of nodes because there is no need to update the network's mode manually when adding new nodes. In general, the self-organization characteristic of WSN makes WSN more reliable as network reconstruction can be achieved in real-time mode, allowing the WSN to rapidly react to the environment changes or sensor node failures. Furthermore, algorithms of self-organization can provide optimization of data transmission power usage.

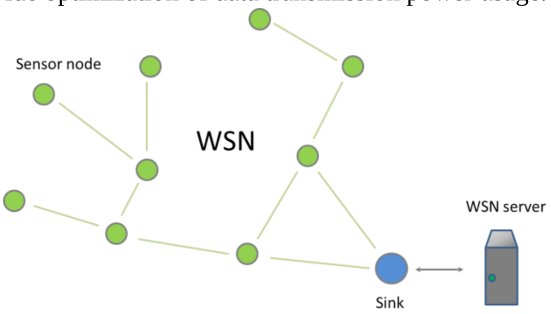

Fig. 1: Example of Wireless Sensor Network

This chapter reviews briefly different scheduling algorithms for WSN. An OGC Sensor Web Enablement (OGC-SWE) is a sort of sensor network that is suited for environmental monitoring. Zigzag scheduling scheme [1] increases OGC-SWE's slow reaction during emergency tasks. This scheduling algorithm is intended to alter the order of execution for the sensor planning service. The required tasks are performed to provide a quick response time depending on the frequency use of sensors. The energy efficient covering problem is solved by the ant colony based scheduling algorithm (ACB-SA) via a realistic approach. In heterogeneous sensor set [2], the probability sensor detection model is used. The optimum amount of active sensor nodes and fusion center is determined to enhance the network lifetime. The data collected by sensors are quantified into texts and then forwarded to the fusion center where the degree of assurance is based on the final estimation [3].

Revised Manuscript Received on 30 July 2019.
* Correspondence Author

Dr.S.J.Subhashini*, Associate Professor, Department of Computer Science and Engineering, K.L.N. College of Information Technology, Pottapalayam, Tamilnadu, India. (E-mail: subha1472@gmail.com)

Dr.B.Stalin, Assistant Professor, Department of Mechanical Engineering, Anna University, Regional Campus Madurai, Madurai-625 019, Tamilnadu, India. (E-mail: stalin1312@gmail.com)

Mr.J.Vairamuthu, Research Scholar, Department of Mechanical Engineering, Sethu Institute of Technology, Kariapatti, Virudhunagar Dist., Tamilnadu, India.

The dynamic multilevel priority packet scheduling system for wireless sensor networks ensures minimal end-to-end data transmission. This system has better efficiency in terms of an average job waiting for the time and end to end delay than the current FCFS and multi-level queue scheduling. Tasks that have expired deadlines are removed to decrease the overhead processing and save bandwidth [4]. Clustering protocol based on an energy-efficient position divides the network region into distinct levels. Cluster heads are created in the growing order at each stage. The cluster heads near the base station are tiny in size and use round robin to forward the information to the base station. This protocol improves the performance in delay and energy consumption [5]. The integration of wireless sensor network and mobile cloud computing is the best research topic in both academic and industry. In this paradigm, wireless sensor network offers reliable data to the cloud and mobile users demand data from the cloud [6]. The TPSS–named WSN-MCC Scheme saves energy consumption and more reliably transmits information. TPSDT will selectively transmit data to the cloud depending on the data required by the mobile user's time and priority [7].

WerMDG considers different sources of energy consumption and different time factor for energy replenishment. It is carried out in a distributed manner [8]. Joint time slot power control and rate assignment problems are considered [9]. Through this optimal throughput is achieved. Only sensing units are examined in a wireless sensor network with various bearings. The adaptive strategy is discussed to schedule the above-mentioned network. To maintain the tracking error below a certain threshold, a minimum amount of readings is determined for each node. The scheme shows the proposed method results in less RMS position error than the nearest node selection method.

II. System Architecture

The following Figure 2 shows the system architecture diagram for the data injection and Byzantine attack detection model with priority scheduling.

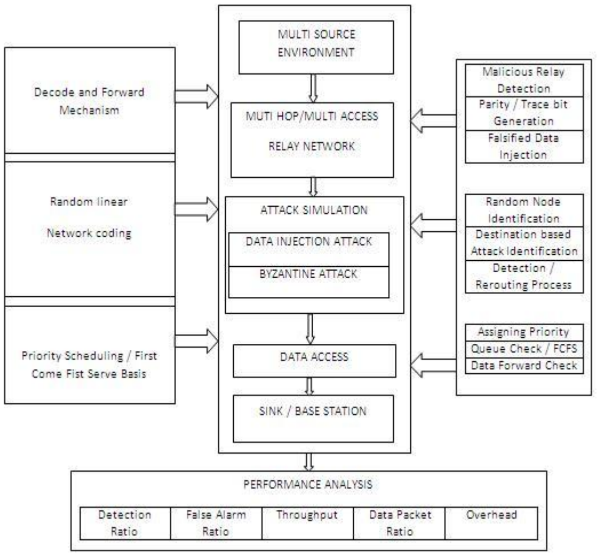
MULTI SOURCE ENVIRONMENT
Decode and Forward Mechanism
MUTI HOP/MULTI ACCESS RELAY NETWORK
Malicious Relay Detection
Parity / Trace bit Generation
Falsified Data Injection
Random linear Network coding
ATTACK SIMULATION
DATA INJECTION ATTACK
BYZANTINE ATTACK
Random Node Identification
Destination based Attack Identification
Detection / Rerouting Process
Priority Scheduling / First Come Fist Serve Basis
DATA ACCESS
Assigning Priority
Queue Check / FCFS
Data Forward Check
SINK / BASE STATION
PERFORMANCE ANALYSIS
Detection Ratio
False Alarm Ratio
Throughput
Data Packet Ratio
Overhead

Fig. 2: Data Injection and Byzantine Attack Detection with Priority Scheduling – Architecture Diagram

The following Figure 3 shows the data flow diagram for data injection and Byzantine attack detection with priority scheduling model.

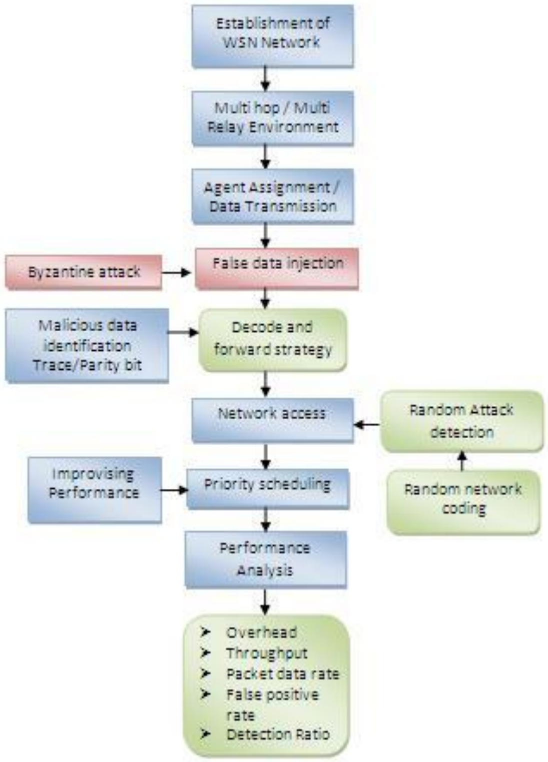

Fig. 3: Data Injection and Byzantine Attack Detection with Priority Scheduling–Data Flow Diagram

III. Modules Description

A wireless sensor network (WSN) comprises of diversely disseminated self-sufficient sensors for the observation of various physical or conservational situations like climatic variations, temperature, pressure variance, etc. Then WSN will share the data within and across the network in a collaborate fashion. Most of the latest wireless sensor networks are two directional, so that proper control of sensor activity is maintained. The wide establishment of wireless sensor networks was largely inspired by various military solicitations like surveillance in the war field, radar monitoring applications, etc. In industrial applications, WSN is used in multi-facet consumer-oriented provinces such as automatic process control, health monitoring, security mechanisms etc.

Decode-and-Forward Strategy

The threshold may be selected to obtain a target false alarm, error detection, or error probability. We exploit the detection outcome to improve the reliability of decoding by erasing (discarding) the data received from the adversarial nodes and correcting the erasures. The fact is that erasures can be corrected twice as many as errors. Nevertheless, the information in the presence of attack scenario may not be impeccable in real time situations.

The false alarm results in an erasure of correct bit, while the miss detection may result in an error in place of an erasure. As the probability of false alarm and that of miss detection based on the amount of tracing bits and the errors-and-erasures correction capability based on the number of parity bits, we suspect there exists an optimal allocation of the redundancy between tracing bits and parity bits that reduces the probability of decoding error at the destination. Here, the tracing random bits are to find the malicious relay nodes and erase the data received from them, while the parity bits are to correct errors caused by channel and noise. Larger parity bits with high accuracy infer lower tracing bits with less security with the specified redundancy rate. The reverse also holds good**.**

Network Coding

A serious risk to wireless sensor networks is the Byzantine attack in which the adversary has complete control over some of the authenticated nodes and can perform the arbitrary behavior to disrupt the system. Network coding is a method that enables intermediate nodes to encode data packets obtained from its neighboring nodes in a network. The encoding and decoding methods of linear network coding are outlined below.

Encoding operation: A node, that wishes to send encoded packets, chooses a sequences of coefficients $q = (q_1, q_2 ... q_n)$, called encoding vector, from GF (2^s). For a group of n number of packets G_i (i = 1, 2, 3, 4... n) which are received at a node are linearly encoded into a single output packet. The resultant output encoded packet is given by

$$Y = \sum_{i=1}^{n} q_i \, G_i, \quad q_i \in GF(2^s) \qquad (1)$$

The coded packets are transferred using the network's n coefficients. The encoding vector is used at the receiver to decode the encoded data packets.

Decoding operation: A receiver node solves a set of linear equations from the received coded packets to get the original packets. The encoding vector q is acquired by the receiver sensor nodes with the encoded data. Let, a set (q_1, Y_1)..., (q_m, Y_m) has been obtained by a node. The symbols Y_j and q_j denote the information symbol and the coding vector for the j^{th} received packet respectively. A node solves the following set of linear equations for decoding procedure with m equations and n unknowns .

$$Y_j = \sum_{i=1}^{n} q_i^j \, G_i, \; j = 1, \dots, m \qquad (2)$$

The recipients must receive at least n linearly autonomous coded packets for adequate decoding of the initial packets. The only unknown, *Gi*, consists of original packets that are transmitted in the network. After receiving n linearly autonomous packets, the amount of initial packets can be retrieved by solving the linear model in the equation.

A. Priority Algorithm

The approach aims at adjusting the threshold value which denotes the number of the bandwidth request message in the nrt PS service class. The scheduling scheme begins with the scheduler visits to rtPS. The rtPS is maintained until no more bandwidth request message is available. Before continuing the service to nrtPS, the scheduler will examine the amount of bandwidth request available in the nrtPS service class. If the amount of bandwidth request exceeds the threshold assigned, then the scheduler will perform the service to nrtPS and subsequently the BE. Alternatively, the scheduler will go back to the service rtPS, provided the count of bandwidth request is smaller than the threshold allotted.

B. First Come, First Served Scheduling Algorithm

The first come, first served scheduling algorithm is the simplest packet scheduling algorithm in which packets are processed when they arrive. It is the traditional technique used to promote communication in real time. But if many sensor nodes generate data at the same time, it takes more time for data packets from nodes far from the base station to reach the base station than those from nearby nodes. We should therefore consider scheduling the delivery order of the data packet within a deadline in instant nodes. Wireless sensor networks are typically implemented across a broad range of areas and consist of big amount of random nodes. This makes scheduling a major concern. Every node must decide which packet is urgent to communicate data in real time. If there is a deadline for data delivery of data packet that should also be taken into account when scheduling the delivery order so that the significance of the data is not lost when it reaches the base station.

IV. PERFORMANCE ANALYSIS

Performance analysis incorporates the collection of formal and informal data to help customers and sponsors define and achieve their objectives. Performance analysis shows various measures in terms of the system metrics. Analysis of performance is the front end. To find out what to do, it's what we do. Planning, scoping, auditing, and diagnosis are some synonyms.

Simulation Analysis

The parameters and the values used for the simulation analysis are presented in Table 1.

Table 1: Simulation Environment

Simulation parameters	**Simulation values**
Access Standard	IEEE 802.15.4
Number of nodes	40
Base protocol	AODV
System Bandwidth	2 Mbps
Protocol Layer	Cross-Layer MAC
Antenna	Omni Directional
Simulation Environment	1500 * 1500
Channel Propagation	Wireless / Two ray ground
Problem Statement	Identification of data injection attack / Byzantine Attack
Algorithms	Decode and Forward Mechanism, Random Linear Network Coding
Improvisation	Priority Scheduling

Figure 4 shows the simulation analysis of the packet data ratio vs. simulation time. From the simulation analysis, it is inferred that the packet data ratio for the optimal scheduling mechanism has the better output results when compared with the existing data injection algorithm, byzantine attack detection algorithm and normal data flow in wireless sensor networks.

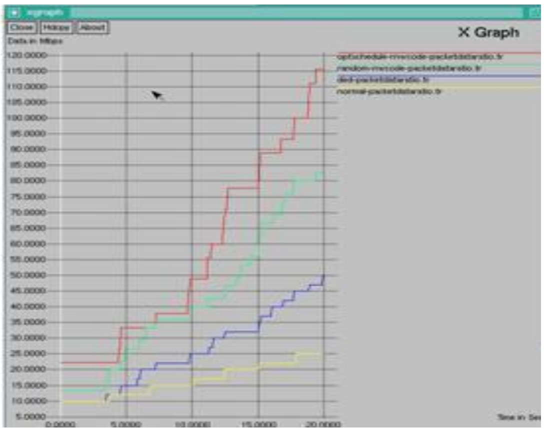

Fig. 4: Simulation Analysis – Packet Data Ratio Vs Time

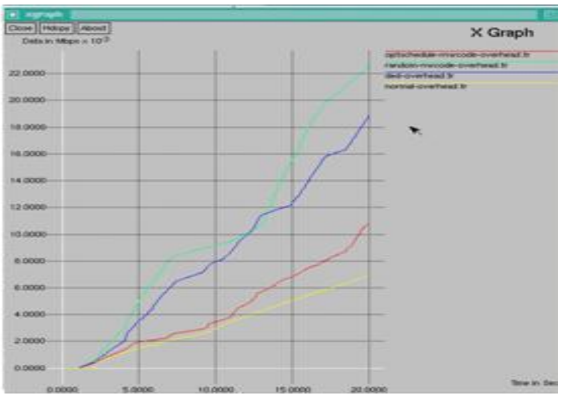

Fig. 5: Simulation Analysis – Overhead Vs Time

Figure 5 shows the simulation analysis of overhead vs. simulation time. From the simulation analysis, it is inferred that the packet data ratio for the optimal scheduling mechanism has the better output results when compared with the existing data injection algorithm, Byzantine attack detection algorithm and normal data flow in wireless sensor networks.

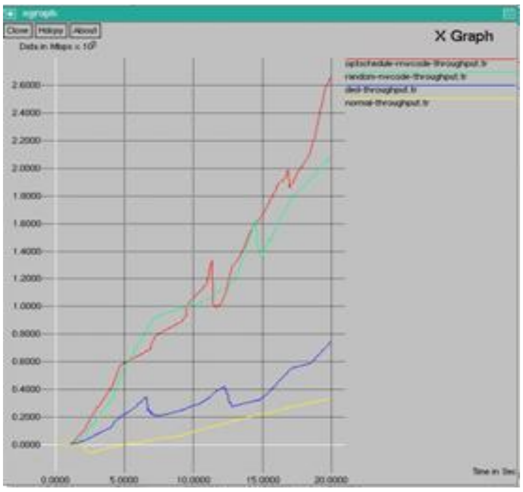

Fig. 6: Simulation Analysis – Throughput Vs Time

Figure 6 shows the simulation analysis of throughput vs. simulation time. From the simulation analysis, it is inferred that the packet data ratio for the optimal scheduling mechanism has the better output results when compared with the existing data injection algorithm, byzantine attack detection algorithm and Normal data flow in wireless sensor networks.

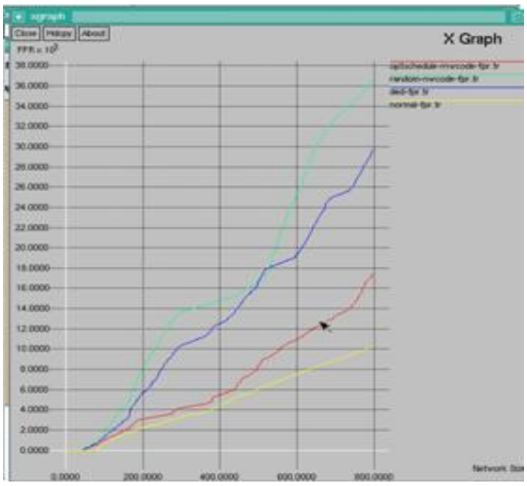

Fig. 7: Simulation Analysis – False Positive Ratio Vs Time

Figure 7 shows the simulation analysis of the false positive ratio vs. simulation time. From the simulation analysis, it is inferred that the packet data ratio for the optimal scheduling mechanism has the better output results when compared with the existing data injection algorithm, Byzantine attack detection algorithm and normal data flow in wireless sensor networks.

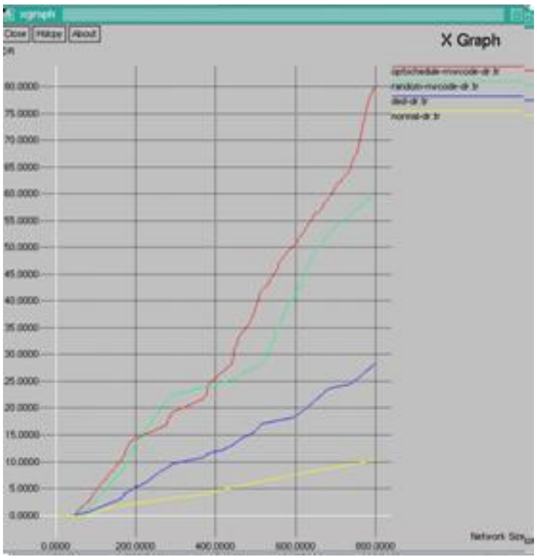

Fig. 8: Simulation Analysis – Detection Ratio Vs Time

Figure 8 shows the simulation analysis of the detection ratio vs. simulation time. From the simulation analysis, it is inferred that the packet data ratio for the optimal scheduling mechanism has the better output results when compared with the existing data injection algorithm, Byzantine attack detection algorithm and normal data flow in wireless sensor networks. In addition to the simulation analysis, the following comparative analysis is shown for multi-relay sensor network reliability and security.

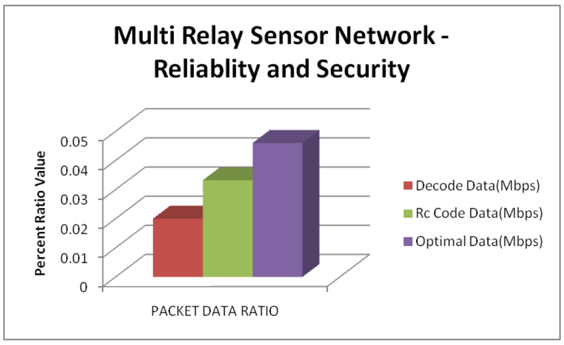

Fig. 9: Comparison Analysis – Packet Data Ratio

In the comparison analysis Figure 9, for the parameter packet data ratio with the x coordinate and the y coordinate values, percent ratio value vs. packet data ratio, optimal data values have better results when compared to decode data and Rc code data.

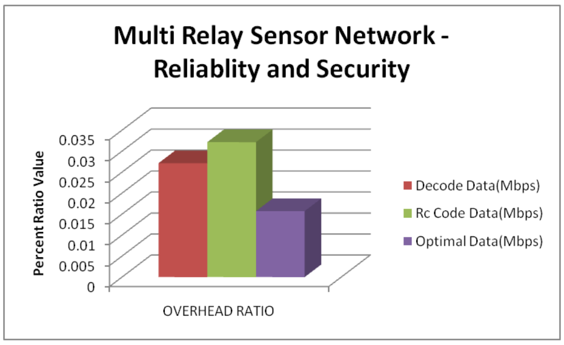

Fig. 10: Comparison Analysis – Overhead Ratio

Similarly, in the comparison analysis Figure 10, for the parameter overhead ratio with the x coordinate and the y coordinate values, percent ratio value vs. overhead ratio, optimal data values have better results when compared to decode data and Rc code data.

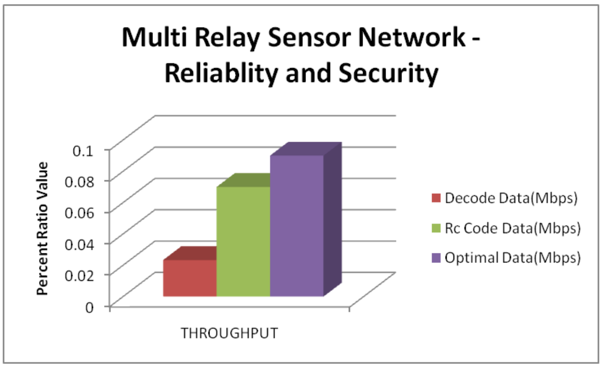

Fig. 11: Comparison Analysis – Throughput Ratio

In the comparison analysis Figure 11, for the parameter throughput ratio with the x coordinate and the y coordinate values, percent ratio value vs. throughput ratio, optimal data values have better results when compared to decode data and Rc code data.

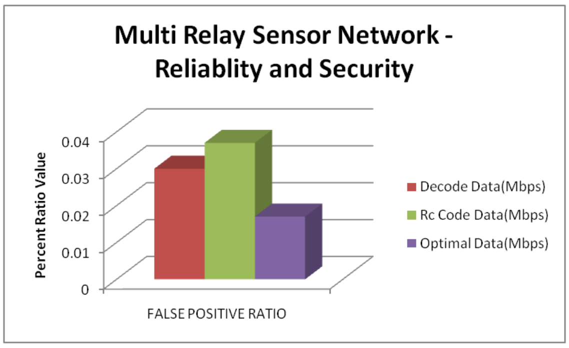

Fig. 12: Comparison Analysis – False Positive Ratio

In the comparison analysis Figure 12, for the parameter false positive ratio with the x coordinate and the y coordinate values, percent ratio value vs. false positive ratio, optimal data values have better results when compared to decode data and Rc code data.

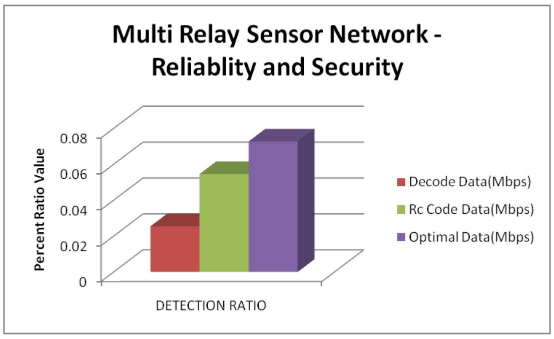

Fig. 13: Comparison Analysis – Detection Ratio

In the comparison analysis Figure 13, for the metric detection ratio with the x coordinate and the y coordinate values, percent ratio value vs. detection ratio, optimal data values have better results when compared to decode data and Rc code data.

V. CONCLUSION AND FUTURE WORKS

In our work, the practical approach of detecting data injection and Byzantine attacks using the proposed method of random network coding is performed. Then, as improvisation measure, the priority scheduling algorithm is implemented to effectively schedule the transfer of data. Our proposed structure acclimatizes well to the exponentially growing needs of wireless sensor networks in heterogeneous applications. The priority scheme programs real-time measures with the topmost precedence guaranteeing least end-to-end data delay and better packet delivery ratio and throughput. The scheme also plans least precedence measures with impartiality so that their delivery ratio is also not affected. Simulation results using the NS2 environment show that using the priority scheduling algorithm has good performance values in terms of the packet delivery ratio, throughput and delay. In addition to that, the attack detection metrics such as false positive ratio and detection ratio are also upgraded when using the priority scheduling algorithm.

Thus a updated priority algorithm for an uplink scheduler in WSN is implemented to increase the performance and detection metrics. As future work, the heterogeneous sensor networks can be integrated and attack detection model with priority scheduling can be suggested as the future work in this domain. It is also possible to develop sensor web and sensor grid architectures and cloud based architectures for sensor networks. These attack detection models with scheduling path can be much useful one. The heterogeneous applications will identify real-time usage in future information based data communication. Also, in addition to the attack detection and scheduling, data aggregation and middleware framework can be implemented in the wireless sensor network.

ACKNOWLEDGMENT

We thank the management of K.L.N. College of Information Technology, Pottapalayam, Tamilnadu, India for providing us enough resources to prepare and experiment our work. We are thankful to our faculty members and staffs for their support.

REFERENCES

1. Chang-Han Kwon, Ki-Hyung Kim and Seung-WhaYoo, “A Zigzag Scheduling Scheme for Properties of Sensor Task based on OGC Sensor Planning Service,” IEEE 5th International Conference in the 2010 Proceedings of the Ubiquitous Information Technologies and Applications, Dec. 2010.
2. Joon-Woo Lee and Ju-Jang Lee (2012), Ant-Colony-Based Scheduling Algorithm for Energy-Efficient Coverage of WSN. *IEEE sensors Journal12(10)*, pp. 3036-3046.
3. Amir Hossein Mohajerzadeh, Mohammad Hossein Yaghmaee, Vahid Fakoor and Elham Mirfarah,“Optimum Routing and Scheduling for Estimation in Wireless Sensor Networks,” Second International Conference on Computer and Knowledge Engineering (ICCKE), October 18-19, 2012.
4. Nidal Nasser, Lutful Karim and Tarik Taleb (2013), Dynamic Multilevel Priority Packet Scheduling Scheme for Wireless Sensor Network.*IEEE Transactions on Wireless Communications 12(4)*, pp. 1448-1459.
5. Itika Gupta and A. K. Daniel, “An Energy-Efficient Position Based Clustering Protocol for Wireless Sensor Network Using Round Robin Scheduling Technique,” Third International Conference on Advanced Computing & Communication Technologies, 2012.
6. Chunsheng Zhu, Zhengguo Sheng, Victor C. M. Leung, Lei Shu and Laurence T. Yang (2015), Towards Offering More Useful Data Reliably to Mobile Cloud from Wireless Sensor Network.*IEEE Transactions on Emerging Topics in Computing3(1)*, pp. 84-94.
7. SongtaoGuo, Cong Wang, and Yuanyuan Yang (2014),Joint Mobile Data Gathering and Energy Provisioning in Wireless Rechargeable Sensor Networks.*IEEE Transactions on Mobile Computing13(12)*, pp. 2836-2852.
8. Y. Alayev, F. Chen, Y. Hou, M. P. Johnson, A. Bar-Noy, T. La Porta and K. K. Leung, "Throughput maximization in mobile WSN scheduling with power control and rate selection", In Proc. IEEE 8th Int. Conf. Distrib. Comput. Sensor Syst., 2012, pp. 33-40.
9. Nayebi-Astanesh, N. Pariz and M. B. Naghibi Sistani (2015), Adaptive Node Scheduling Under Accuracy Constraint for Wireless Sensor Nodes with Multiple Bearings-Only Sensing Units. *IEEE Transactions on Aerospace and Electronic Systems 51(2)*, pp. 1547-1557.

AUTHORS PROFILE

Dr.S.J.Subhashini, working as a Associate Professor of CSE department in K.L.N. College of Information Technology, Pottapalayam, Tamilnadu, India. She has completed her Ph.D in Anna University Chennai. She has more than 15 years of experience. Her areas of interest include data mining, image processing, wireless networks and cloud computing.

Dr.B.Stalin received B.E. Degree in Mechanical Engineering from the University of Madras, Tamilnadu, India and M.E. Degree in Manufacturing Engineering from the Anna University, Tamilnadu, India. He obtained his Ph.D. in Mechanical Engineering discipline at Anna University, Chennai, Tamilnadu, India. His current research interests include Materials Characterization, Mechanical Properties, Composite Materials, Optimization Techniques, and Manufacturing Engineering.

Mr.J.Vairamuthu received B.E. Degree in Production Engineering from the Sethu Institute of Technology, Pulloor, Kariapatti, Tamilnadu, India and M.E. Degree in Engineering Design at Anna University, Regional Campus Madurai, Tamilnadu, India. He has more than 10 years of experience. His current research interests include Materials Characterization, Mechanical Properties, Composite Materials, Corrosion and Additive Manufacturing.