I J C T A, 9(7), 2016, pp. 3053-3060 ISSN: 0974-5572
© International Science Press

An Efficient Approach for Packet Dropping Detection Using PGLP with Trace Back Mechanism

Priyanka* and M. Devika**

ABSTRACT

In WSN sensor network are very closely and densely deployed with respect to various applications and domains, the gathering data are forward vis-à-vis with adversary nodes used in decision finding the critical scenarios. Gathered data are forwarded to innumerable sources through intermediate handling nodes in order to diminish the packet dropping attacks, in this paper introduced the PGLP based trace back mechanism to eradicate and solve the attacks and false positive ratio. With the help of PGLP based route exploits its well decision making in the communication context to particularly drop a various routes, hence this mechanism to strengthen the security of data, collusion proof, and incurs low communication and storage overheads. In addition, we encompass the safe origin scheme with functionality to detect packet drop attacks caused by malicious data forwarding nodes. We evaluate the proposed technique both critically and empirically, and the consequences demonstrate the efficiency of the packet loss attacks with forgery attacks.

Keywords: Packet Drop Attacks, WSN, PGLP, Trace back Mechanism

1. INTRODUCTION

Wireless Sensor Networks are used in functional domains which occur both tracking and monitoring system. Data packet are transmitted alone the sensor network, the nodes and base station between source to destination perform decision making operation. Sensor network property is to transmit the data packet confidentiality, securely, freshness, and time management and secure localization. In recent research [1] on provenance in system where the use of unreliable data may lead to disastrous failure. We examine the problem of safe and efficient provenance transmission and processing for sensor networks, and we use provenance to spot packet loss attacks staged by malicious sensor nodes. In a multi-hop sensor network, data provenance allows the BS to trace back the source and forwarding path of an individual data packet.Tracing each source and forwarding path, it improve the challenges of the sensor network such as compact storage, energy usage and bandwidth consumption. In addition sensors are operated in an untrusted environment, where they may be subject to attacks. Our objective is to design a provenance encoding and decoding mechanism to satisfy such security, performance needs and trustworthiness of the provenance by reducing usage of energy.

In existing work, securely set provenance information within a bloom filter (BF) also transmitted. Upon receiving the packet, the base station (BS) finds and verifies the provenance information. That permit the BS is to find if a packet drop attack was occurred by a malicious node. In proposed work main aim to give trust to the network by using routing protocol. It uses the single transmission channel for both data and provenance. Here it focuses on both security and trustworthiness for the network. It provide secure provenance scheme, and improves packet delivery rate, and it prevent the packet to enter in the malicious node. As

* M.Tech (VLSI), Sathyabama University, Chennai, *Email: priyankasbu2024@gmail.com*

** Assistant Professor, Sathyabama University, Chennai, *Email: devikadivya28@gmail.com*

opposed existing system separate transmission channels used for data and provenance. The main motive is to reduce the pcket drop attack in wireless sensor network by changing the path in network or by dropping the malicious node which is present in the network. So to achieve the goal of the project here using the PGLP mechanism. Which help to get a shortage and secure path for transmission. But in our project we required only a single transmission channel for both data and provenance.

In addition, traditional secureprovenance solutions use intensively cryptography and signatures, and they utilize append-based data structures to store provenance, leading to prohibitive costs. But in our project we use only fast message authentication code (MAC) schemes and Bloom filters make effective usage of bandwidth, and they give low error rates in practice.

LRU replacement algorithm [1], Recursive solution for computing the current score from its provenance [2], hamming metric algorithm [3], AM-FM (authentication manifest and Flajolet-Martin) algorithm [4], provably secure hierarchical in network data aggregation algorithm [5], cryptographic algorithm [6], polynomial–time near– optimal[7], centric routing algorithm [8].

Several authors have proposed various protocols to find packet manipulations, based on endorse the traffic transmitted by one router is received unmodified by one more [2-5], All the proposed algorithms struggle in interpreting the absence of packet dropping attacks, during the packet transfer, that the packet has been altered or during the communication, such a clear proof of interfere, a dropped packet is naturally vague. Since it has been clearly jammed by cooperation router or it might be plunged gently due to network clogging.

This paper is structured as tag along In Section 2 we have another look at the associated work. The structure/opposition replica and problem statement are portrayed in Section 3. The proposed plan and design to analysis its safety measures presentation and outlay in Section 4. Results are well explained in Section 5, and we conclusion of the paper in Section 6.

2. RELATED WORK

Based on detection algorithm provides the communication interaction between original node to malevolent nodes, in order to classify the prior works in following ways.

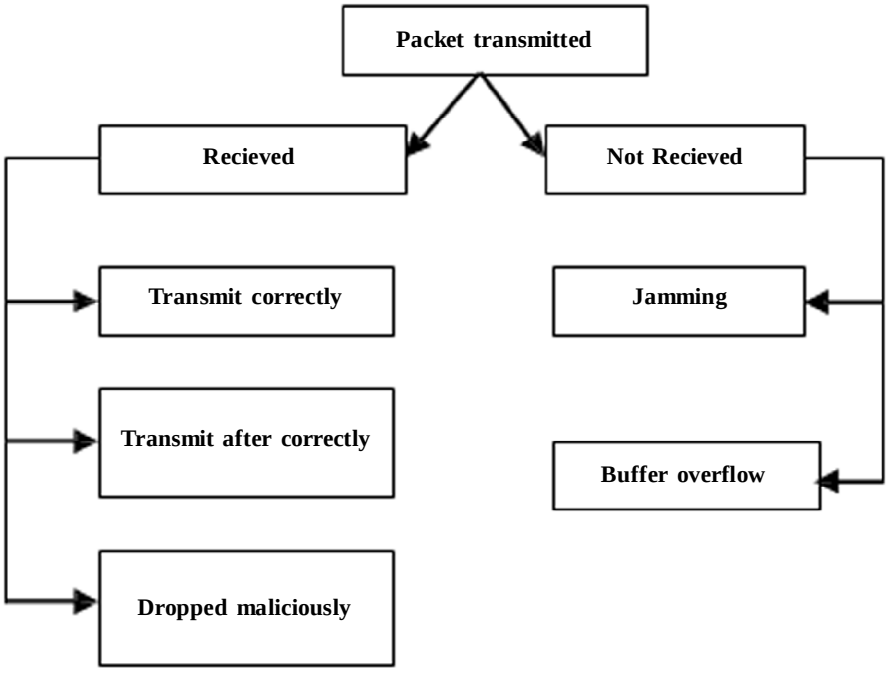

Figure 1: Overview of Packet Loss

Li Fan proposed Two factors of the protocols which have low overhead[1] the summaries are updated only periodically, and the directory representations are very efficient, as low as 8 bits per entry. The algorithm used in this paper is LRU replacement algorithm. Hyo Sang Lim Yang, Sae Moon and Elisa Bertino [2] proposed a cyclic framework which well reflects the inter-dependency property. Experimental results explains and provides less trustworthiness assessment in sensor networks. Algorithm used in this paper is recursive solution for computing the current score from its provenance. Adam Kirsch and Michael Mitzenmacher [3] anticipated distance sensitive bloom filters and the algorithm used in this paper is hamming metric. Minos Garofalakis, Joseph M. Hellerstein, and PetrosManiatis[4] In this paper they consider the problem of ensuring verifiable however efficient results to typical aggregation queries in a distributed, multi-hop setting. We explain a framework for the problem, including the threat Model for adversaries that we review. We then present a mechanism called a proof sketch, which uses a compress combination of cryptographic signatures and Flajolet-Martin sketches to solve that a query answer is within acceptable error bounds with high probability. The algorithm used in this paper is AM-FM (authentication manifest and Flajolet-Martin). Haowen Chan, Adrian Perrig and Dawn Song [5] in this they present the algorithm for provably protected and safe hierarchical in network data aggregation. Here algorithm is gives surity to detect any manipulation of the aggregate by the adversary beyond what is achievable through straight injection of data values at compromised nodes. Hani Alzaid, Ernest Foo and Juan Gonzalez Nieto [6] in this dataaggregation technique are introduced. Algorithm used in this paper is cryptographic algorithm. KoustuvDasgupta, KonstantinosKalpakis and ParagNamjoshi [7] in this a key challenge in data gathering is used to maximize the system lifetime, given the energy constraints. In this a polynomial– time near–optimal algorithm is used for solving the maximum lifetime data gathering (MLDA) problem for sensor networks. Chris Karlof and David Wagner [8] put forward to strengthen for course-plotting in sensor networks; its show that how efficient attacks against ad-hoc and peer to peer large scale networks can be adapted into powerful attacks against sensor networks and the algorithm used in this is data centric based routing algorithm has been used.

3. SYSTEM MODEL

3.1. Network and Channel Models

Consider a arbitrary path in wireless sensor network as shown in fig 2. The source node continuously send packet to the destination node through intermediate node. Where source node aware of the route as in Dynamic Source Routing (DSR) [12]. If DSR are not used to find the route than trace route operation is used to find the route.

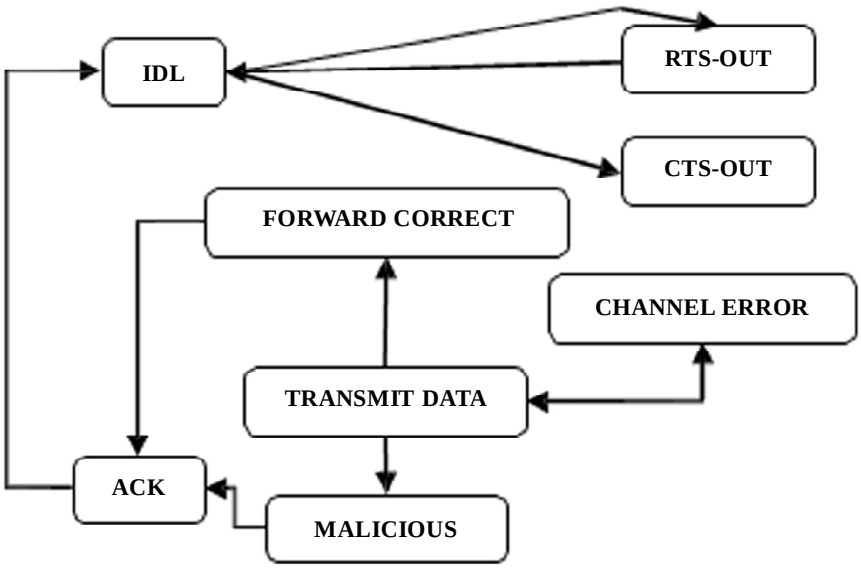

Figure 2: Overview of Trace Route Operation.

3.2. Back Tracking Mechanism

Algorithm 1:

Source extracts src_addr(packet_addr)
next_nodeclosest_next_node(nxt_node)
If(is_neighbour (next_node)) then
Forward(src_node, next_node)
else
next_hop_to_non_neighbour (next_node)
forward (source_node, rx_node)
endif

From this algorithm, the source node extract the packet information starts transmit from source address to next neighbourhood address, if the neighbour node is denoted like next_node, forwarded to next hopping node else it won't transmit to non neighbour nodes, otherwise it will forwarded to destination node.

Notation:

Packet_addr → Pointing the packet Address
nxt_node → Addressing the Next Node
src_node → Representing the origin node
rx_node → indicating the receiver (destination) node.

Algorithm: 2

S = extract_source_address (p)
A = extract_attestation (p)
if (not verify_source_sig(p)) or (empty(a) and not
is_neighbour(s)) or (not saowf_verify(a)) then
return /*drop (p)*/
for all node in a do
prevnode = node
if (not are_neighbours(node, prevnode)) or (not making
progress(prevnode, node))
then
return /*drop(p)*/
end if
end for
end if
c = closest _next_ node(s)
P = saowf_append (p)
If(is_neighbours(c)) thenforward (P, c)2
else
forward(P, next_hop_to_nonneighbor(c))
end if

This algorithm shows workflow of trace back mechanism. It first extracts the source address than check whole network. If any malicious node or unwanted packet find than it will drop. It will check for the neighbornodes which are not involve in transmission than it will dead the node. Than it forward the packet, if any malicious node is present than change the route than transmit the data. Overall it increases the trustworthiness of the network.

4. PROPOSED METHOD

In proposed work, PGLPa based method mainly focused on avoiding DOS attack, packet drop loss, increase packet delivery rate, improve end to end delay analysis and decrease packet drop. Here PGLP prevent the data packet from entering into a malicious node. Hence it defense in contradiction of some of the secure forwarding phase from attacks and described PGLPa. Generally PGLP routing protocol works in two phase topology detection phase followed by packet forwarding phase.

In topology detection phase here it will check the whole network and detect all possible routes from source to destination. During this checking period any malicious node is present in the route, than it will drop the malicious node. In network the node which are not involve in transmission it will dead that that nodes, to minimize the energy usage.

The next phase is forwarding phase, here it check secure shortest path among the entire possible route. Through this it increase the trust of the network while transmission of the packet from source to destination. It will solve the problem beyond the cryptographic. Here the node which are involved in transmission uses DSR source protocol to ensure that the route is valid or not at the time of sending the packet.

5. EXPERIMENTAL EVALUATION

Experimental work on NS2 simulator. The movement of all sensor nodes is formulated over a size of 1500m × 1500m sensor field. NS2 simulation takes 49 sensor nodes for investigation aldetermination with the aid of routing protocol to accomplish the experimentation.

The Figure 3 shows that the successful packet transmission of the existing method, from the graph it canbe observe that the system has shows that packet started from source node to reach the node22 destination node.

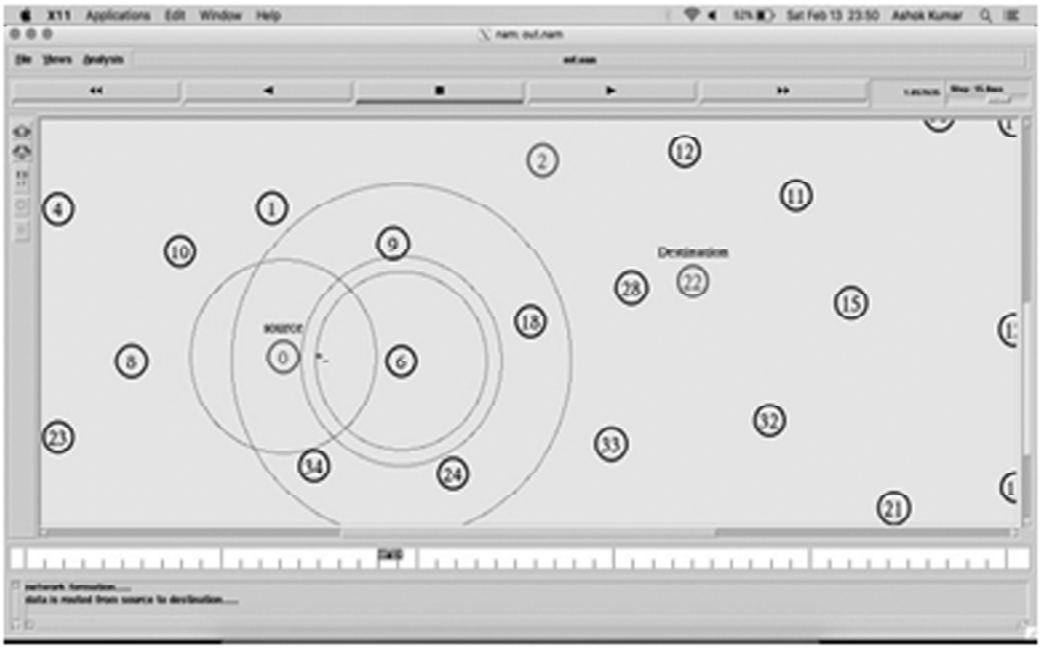

Figure 3: Packet Transmission

The Figure 4 it can conclude that packet drops loss has identified with the assist of proposed system by using trace back mechanism. The packet drop has been identified that node 18 transit the packet to node 28, during that transit loss can be identified with the support of our proposed method.

The Figure 5 describes the successful packet delivery of our proposed system with existing system, from the graph we observe that proposed system has 0.98 as successful delivery rate with respect to pause time, while the existing system has 0.7 as delivery rate from the result we observe that proposed system has high delivery rate.

The Figure 6 describes the end to end delay of our proposed system with existing system, from the graph we observe that proposed system has 2 ms as delay time with respect to pause time, while the existing system has 6.0 ms as delay rate from the result we observe that proposed system has low delay time.

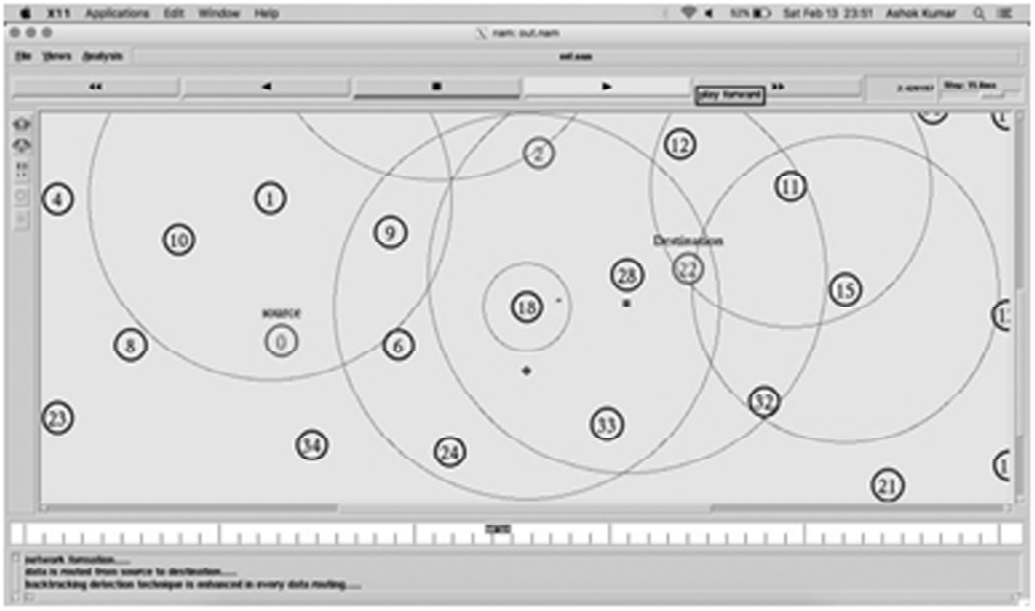

Figure 4: Packet drop attack

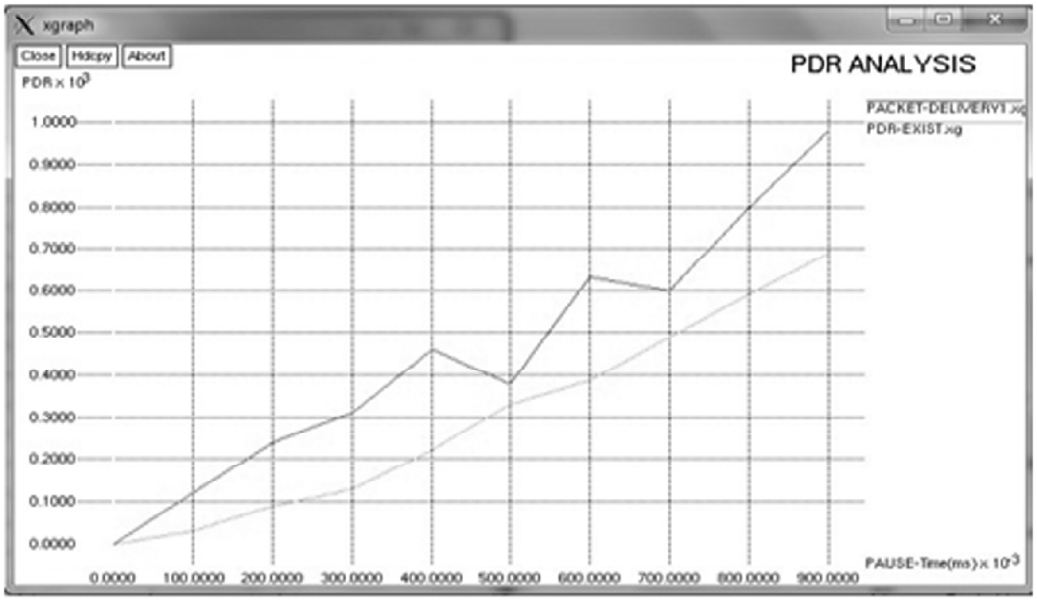

Figure 5: PDR Analysis

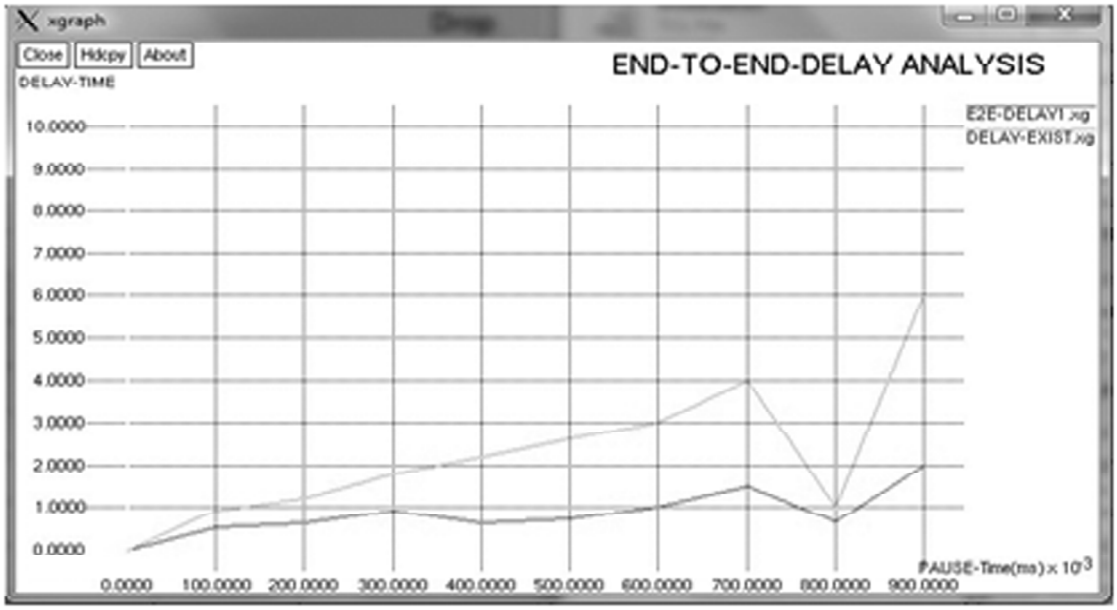

Figure 6: End to End delay

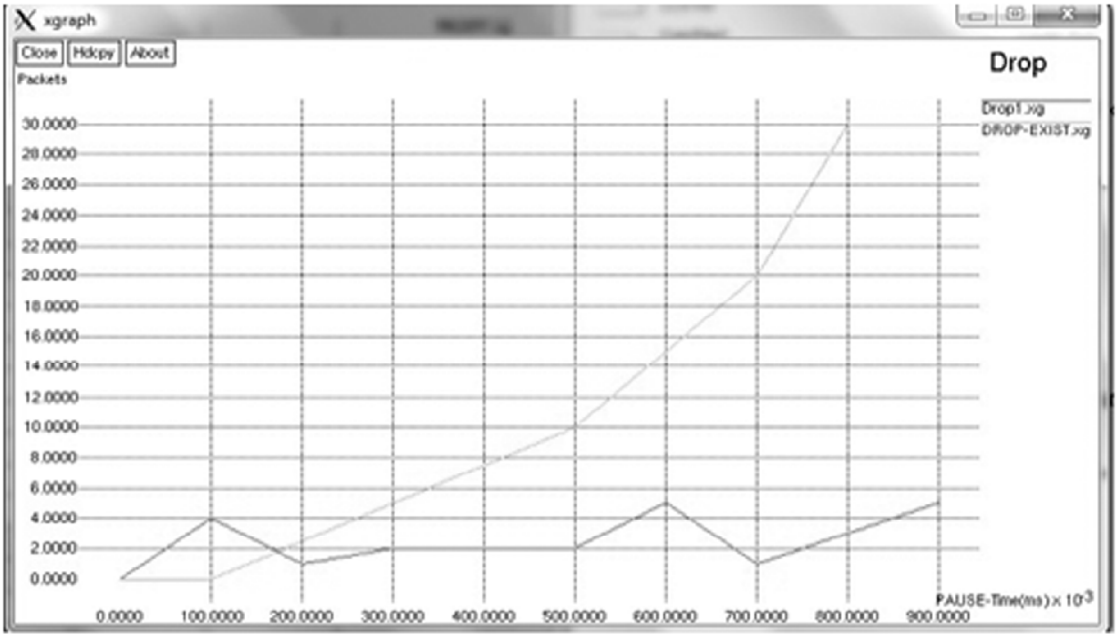

Figure 7: Drop rate

The Figure 7 describes the drop rate of our proposed system with existing system, from the graph we observe that proposed system has 6 packet drop with respect to pause time, while the existing system has 30.0 as drop rate from the result we observe that proposed system has low drop rate.

6. CONCLUSION

In this project, we have proposed and investigated the performance of range free localization for wireless sensor networks. Here we are using the PGLP protocol for efficient transmission of packet to forward node and checking all possible routes in network. In proposed work shows the comparison in term of successful packet transmission, decreased packet drop loss, high packet delivery rate, low drop rate, and low delay time. Here achieving an energy-efficient data transmission mechanism.

REFERENCES

[1] L. Fan, P. Cao, J. Almeida, and A.Z. Broder, "Summary Cache: A Scalable Wide-Area Web Cache Sharing Protocol," IEEE/ACM Trans. Networking, vol. 8, no. 3, pp. 281-293, June 2000.

[2] H. Lim, Y. Moon, and E. Bertino, "Provenance-Based Trustworthiness Assessment in Sensor Networks," Proc. Seventh Int'l Workshop Data Management for Sensor Networks, pp. 2-7, 2010.

[3] A. Kirsch and M. Mitzenmacher, "Distance-Sensitive Bloom Filters," Proc.Workshop Algorithm Eng. and Experiments, pp. 41-50, 2006.

[4] M. Garofalakis, J. Hellerstein, and P. Maniatis, "Proof Sketches: Verifiable In-Netwok Aggregation," Proc. IEEE 23rd Int'l Conf. Data Eng. (ICDE), pp. 84-89, 2007.

[5] H. Chan, A. Perrig, and D. Song, "Secure Hierarchical In-Network Aggregation in Sensor Networks," Proc. Conf. Computer and Comm. Security (CCS), pp. 278-287, 2006.

[6] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure Data Aggregation in Wireless Sensor Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 3, pp. 1040-1052, June 2012.

[7] K. Dasgupta, K. Kalpakis, and P. Namjoshi, "An Efficient Clustering Based Heuristic for Data Gathering and Aggregation in Sensor Networks," Proc. Wireless Comm. and Networking Conf., pp. 1948-1953, 2003.

[8] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. Int'l Workshop Sensor Network Protocols and Applications, pp. 113-127, 2003.

[9] Tao Shu& Marwan Krunz, "Detection of Malicious Packet Dropping in Wireless Ad Hoc Networks Based on Privacy-Preserving Public Auditing", WiSec'12, April 16–18, 2012, Tucson, Arizona, USA.

[10] M. Kirankumar, A. Sai Harish, "A Novel Schema for Detecting Malicious Packet Losses", International Journal of Modern Engineering Research (IJMER).

[11] Thaier Hayajneh, Prashant Krishnamurthy, David Tipper, and Taehoon Kim, Detecting Malicious Packet Dropping in the Presence of Collisions and Channel Errors in Wireless Ad hoc Networks, IEEE Transaction,2009.

[12] J.H. Yun and S.W. Seo, Novel collision detection scheme and its applications for ieee 802.11 wireless lans, Computer Communications, vol. 30, no. 6, pp. 1350–1366, 2007.

[13] Nahur Fonseca and Mark Crovella, "Bayesian Packet Loss Detection for TCP", INFOCOM 2005

[14] S. sultana, G. Ghinita, E. Bertino, and M. Shehab, "A lightweight secure scheme for detecting provenance forgery and packet drop attacks in wireless sensor networks," IEEE Transactions on Dependable and Secure Computing, vol. 99, 2014.