Secured On-Demand Adaptive Routing (SOAR) Protocol for Data Transmission in IoT Environment

P. Deepavathi and C. Mala

Abstract The emerging concept Internet of Things (IoT) has the capability to communicate data among devices throughout the entire world without human intervention. Existing reactive routing-based protocol needs tremendous bandwidth, consumes more processing time and generates large number of control packets for communication. This chapter proposes an efficient Secured On-demand Adaptive Routing (SOAR) protocol for IoT environment with secured data transmission among nodes. The proposed protocol is simulated and tested by using NS2 simulators. The simulation results show that throughput and packet delivery ratios are better than existing protocols.

Keywords Adaptive routing · Secured transmission in IoT · Routing in IoT · IoT

1 Introduction

Internet of Things plays an essential position in developing smart e-health, business, agriculture, home and learning, etc. Professional applications of IoTs are industrial automation, supply chain management, logistics handling, smart transportation, remote sensing and monitoring applications. Especially, Industry 4.0 brings lot of innovations in IoT field, for example, this industry 4.0 is manless automation and data exchanges in manufacturing technologies. It brings smartness in all areas, for example, smart city, smart home, smart office.

Internet of Things is activated with lot of sensors; all sensors are connected with each other. Each sensor collects information and passes to the next one through a lot of intermediate nodes. These nodes use limited power and dynamic network environment. Here, all the nodes are connected through wireless links. Whether the

P. Deepavathi (✉) · C. Mala
Department of Computer Science and Engineering, National Institute of Technology, Tiruchirapalli, Tamil Nadu, India

A. Haldorai et al. (eds.), *3rd EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing*, EAI/Springer Innovations in Communication and Computing, https://doi.org/10.1007/978-3-030-78750-9_15

communication may be wired or wireless, the communications should be secured between the IoT nodes. In the IoT network, routing plays an important role; the major problems in routing are route breaking, traffic, packet loss, and breaching data. In this chapter, the proposed mechanism focuses on secure data transmission between the sender and the receiver.

Some of the security goals that should be achieved during transmission for avoiding attacks on data and network resources are discussed [17]. The secured routing is very important to make secure communication between devices; to enable secure communication, various types of secured routing protocols are proposed. The routing protocols are configuring routing information and identifying the available routes and creating the routing table. The purpose of routing protocol is exchanging routing information among routing devices. Two categories of protocols are used in IoT routing environment [17].

1.1 Proactive-Based

These protocols follow the table-driven approach, where all the routing information is entered in the routing table, which is available in each router in the network. Routing table in this method is fixed; when any changes occur in the neighbour router, that routing table will be modified. Examples are: Optimized Link State Routing Protocol, Destination Sequenced Distance Vector Routing Protocol.

1.2 Reactive-Based

These protocols follow the on-demand based approach, which is the route to be discovered when needed. Therefore, no fixed routing table is in the router; the router will take decision based on the requirements. Example: Ad hoc On-demand Distance Vector and Dynamic Source Routing protocols.

The high- and low-rate attacks affecting the requested services in connectionless environment are explained well in [18]. The different types of attacks possible in Ad hoc On-demand Distance Vector Routing protocols are explained well in [17]. The existing Dynamic Source Routing (DSR) protocol is on-demand route request protocol. This protocol will find the path when a source node wants to communicate with some other node. So, maintaining fixed routing table is not needed. But, DSR protocol will not take care of damaged link, and it is not suitable to vast networks. DSR protocol consumes high bandwidth and large number of resources to complete the task. This protocol is suitable for static environment and small networks. The performance of DSR protocol will be decreased when the path length is increased. Various types of incoming traffic also affect the routing where eliminating the traffic to avoid attacks and improving the Quality of Services are discussed well [19].

The remaining portions of this chapter are structured as follows: Sect. 2 gives more detail about related work. The detailed processes of working methodologies are explained in Sect. 3. The Simulation Results and Performance Analysis are given in Sect. 4. Finally, the proposed method concludes with Sect. 5.

2 Related Work

In this part, security problems under routing protocols under Internet of Things (IoT) have been surveyed. A lot of existing methodologies do not satisfy the current requirements and problems in routing protocols. The following section covered the secure routing protocols used in the IoT environment.

Rahul and Sujata have explained about various advantages, challenges in IoT and listed the factors that affect the routing process. CupCarbon simulator was used for the simulation process. But, this process only deals with static routing. The dynamic routing and also the implementations are very difficult [1]. Sathya et al. proposed Real Time Secure Route Analysis (RTSRA) method for providing Mobile Ad hoc Network routing security. This technique considered lot of factors for making security between source and destination. The author used two types of measurements to calculate metric value for counting number of nodes in the route. This method concluded with a single route for improving the Quality of Service. The main drawback is that if a single route fails, no further communication will occur [2].

Ahamed, Sauf proposed Energy Efficient Geographic (EEG) protocol for avoiding region problems and also balancing the energy maintenance of the concerned networks. This method is finding the single hop nearest node knowledge for forwarding data packets. If suppose the nearest node is malicious node, then all nodes will be hacked easily [3]. Michele, Salma et al. proposed Distributed Learning Algorithm for routing configurations; this concept dealt with only local communications among all the nodes in networks [4]. In this paper, the author proposed Secure Multipath Routing Adhoc (SMRA) protocol where two types of approaches are considered for finding the factors that are affecting the performance of routing. But, time efficiency was not considered [5].

Sharma KP et al. proposed signal control and balancing the load of routing. Adaptive load tuning techniques were proposed to achieve good network lifetime, but this method suffered by higher delays during routing process [6]. Kumar V and Kumar A have explained load prevention concepts to achieve good energy level and better throughput, but again this routing mechanism makes higher delays [7]. In this paper, the author has explained Energy-aware and Secure Multi-hop Routing (ESMR) protocol. Here, the author has considered three main phases for splitting network into inner zone and outer zone. So, this proposed technique minimizes the routing overhead. The drawback of this concept is applicable only for WSN and will not be suitable for heterogeneous-based scenarios [8].

S.B.Thigale and R.K.Pandy have explained named data networking-based Cross-layer Attack Resistant Protocol (NCARP) where three basic layers are considered for identifying malicious attackers in VANET. The problem is it is only applicable for Named Data Networking (NDN)-based architectures [9].

Gauya et al. explained S2MCBR scheme for splitting network into different regions, each region has one trust manager for checking the strength of the signal, link capacities and link-related problems and measuring the trust value of different routes. If the trust value calculation has any error, then the security also can be compromised [10]. M.T. Hammi explained about single key cryptography where advanced key sharing approach was used. The single key is easily hacked by unauthorized nodes [11].

Garg et al. proposed fuzzy rule-based concept; this is an extension of AODV for identifying secure route between IoT nodes [12]. B. Hammi et al. explained about the networking based on wireless communications, where spoofing attack frequently occurred [13]. In this paper, the author proposed secure multi-hop routing protocol for establishing secure transactions between IoT devices. This protocol ensures authentication before a new node joins into the group by using multiple layers of authentication; it causes memory overhead to all the nodes in the network [14].

The author proposed trust-aware secure routing framework. This concept is very useful for avoiding selfish attack, on and off attack, collusion and bad mounting attack and conflict activities attack. This method uses two values (0 and 1) for identifying trust. The trust value is 0 means no trust between nodes, trust value 1 means good trust between nodes. But the main drawback in this method is memory overhead and processing time overhead [15].

In this paper, the author explained a lightweight and trust-related routing where Intrusion Detection System (IDS) estimates the trust of one object and computes limited computational resources. Generally two types of disturbances are getting from neighbors that are unreliable neighbors and unreliable observations. Here, the author did not consider the unreliable observation attacks [16].

3 Proposed Work

This proposed Secured On-demand Adaptive Routing (SOAR) protocol belongs to asymmetric cryptography where the hash chain technique is used to check the authentication of packet, and this hash function value is used for passing the updated routing information to the neighbour nodes. If a node is getting any updated routing information, it will check the authentication of each entries of the message.

Digital signature is incorporated with Route Request (RREQ) message. The source node S wants to communicate with Node D. Therefore, Node S transmits Route Request (RREQ) message with Digital Signature to next neighbour node; that node will check the signature, then it forwards to next neighbour node till it reaches the corresponding Destination node D (see Fig. 1).

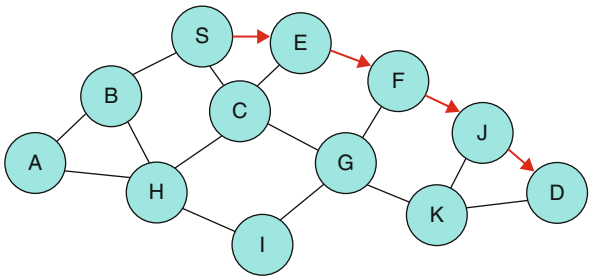

Fig. 1 Route discovery

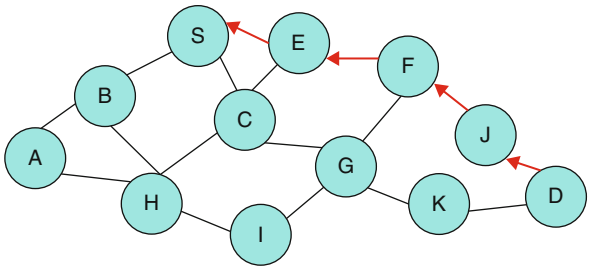

Fig. 2 Route reply

HASHING FUNCTION	MAXIMUM NODE COUNT
BIG HASH	
DIGITAL SIGN	
HASHING VALUE	

Fig. 3 SOAR protocol header

And the corresponding receiver node also will check the signature before producing Route Reply (RREP). The node D sends Route Reply (RREP) message after finding the secure and shortest path (see Fig. 2).

The proposed SOAR protocol header format is shown in Fig. 3. This protocol header has five fields; these fields are doing major functions of checking the authentication and finding secure shortest path for communication among nodes.

In SOAR routing protocol where the hash function is used for ensuring the authentication, it generates the random number that is known as seed. This seed selecting the Maximum Node Count, this maximum node count is used to set the Time To Live value. The Big Hash is used to set the Maximum Node Count Times. While processing RREQ and RREP messages, the hop count hashing with Maximum Node Count checks whether the answer is the same as Big Hash value; if it is same, normal communications continued else the packet is lost. If suppose that link is damaged, the error message will be generated by the nodes (see Fig. 3).

After finds the secure and shortest path, the secure data transmissions will be performed. Here the secure path between S to D is S->E->F->J->D (see Fig. 4).

Algorithm 1 lists the steps involved in SOAR protocol for secure communication among IoT nodes. The notations used in Algorithm 1 are:

N_A = New Node A
N_N = Number of Nodes
G_N = Node Group
S_N = Starting Node
D_N = Receiver Node
I_N = In-Between Node
RREQ = Processing Route Request Message
RREP = Processing Route Reply Message

Algorithm 1: SOAR Routing Algorithm

//Sending and Receiving Route Request and Route Reply

1) New Node N_A Joins with NN in the Network Group G_N
2) Group incremented $G_N=N_N+N_A$
3) Source SN send RREQ to Destination node DN with DIGITAL SIGN
4) Intermediate node IN Check(SIGN(SN))
5) Loop
6) I_N forwards RREQ to next neighbor node
7) $I_N=I_N+1$
8) D_N Received RREQ
9) End Loop
10) D_N Check(SIGN(S_N))
11) D_N send RREP to S_N

//Calculating Shortest and Secure path

12) RREQ and RREP Generate Random Number R_N
13) Repeat
14) R_N=set(MaxNodeCount)
15) MaxNodeCount setting TTL value
16) BigHash=set (MaxNodeCountTimes)
17) OutHash= Hash(MaxNodeCount and MaxNodeCountTimes)
18) If (BigHash == OutHash)
19) Deliver data to the D_N
20) Else
21) Data Packet will be dropped
22) End if
23) End

CupCarbon simulator used in static routing, but it is difficult to implement it in dynamic routing. Real-time Secure Route Analysis methods provide security for single route, but this method is not suitable for multi-hop routes. Secure Multipath Routing Ad Hoc protocol is used for increasing the performance of routing; here, adaptive load-tuning techniques give good energy level and better throughput,

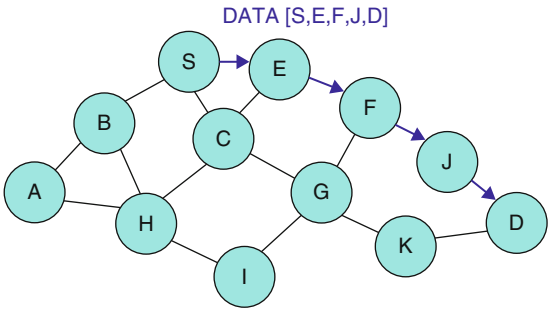

Fig. 4 Secure transmission from source to destination

Table 1 NS2 simulation parameters

Parameters	Values
Runtime	120 s
Coverage region	1000 m * 1000 m
Protocol	DSR
Process interval	0–60s,each step in 20s
Packet load	1000bytes/Packet
Processing speed	200 k
Total nodes	100

but this routing mechanism increased delays. Secure multi-hop routing techniques minimized routing overhead, but this technique is not suitable to heterogeneous networks. Secure multihop routing protocol ensures multiple layers authentication, but it causes memory overhead. These limitations are overcome by this proposed Secured On-Demand Adaptive Routing (SOAR) algorithm. In Dynamic Routing protocol, Hash function is used to provide authentication and Digital Signature is also incorporated in each packet to increase the secure transmission.

4 Simulation Results and Performance Analysis

The Secured On-Demand Ad hoc Routing (SOAR) protocol is simulated by using the NS2 simulator. The following simulation parameters are used for showing the simulation of the proposed protocol (Table 1).

The simulation result of node1 joins in group. Every new node should have proper Digital Signature; after checking the digital signature, it will be added with group G (see Fig. 5).

The performance of sending RREQ message to the neighbor nodes as shown in Fig. 6. In this proposed method, two network groups are doing processes where server1 belongs to one group and server2 is belongs to another group. In the group1 network, lot of nodes are broadcasting route request messages. Each request message is differentiated by different colors.

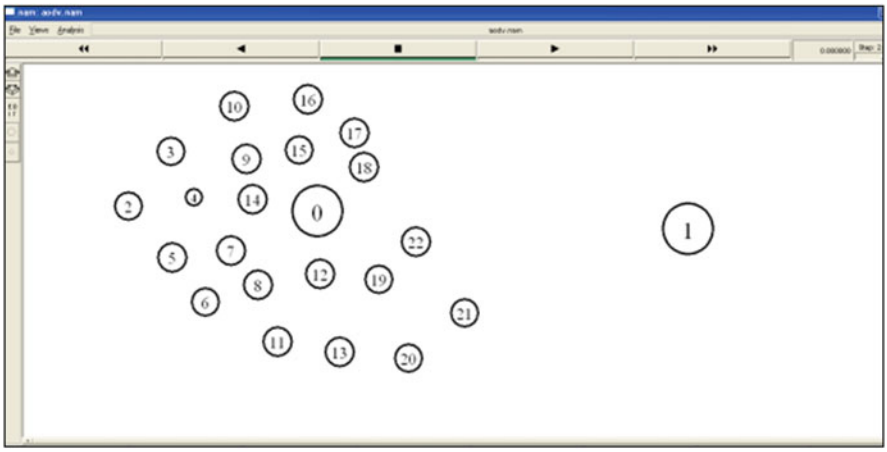

Fig. 5 New node joins

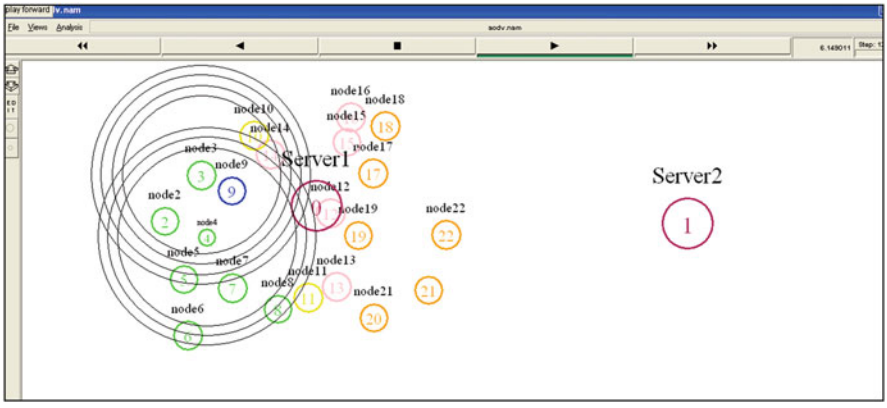

Fig. 6 Broadcasting of RREQ message

The performance of each node is checking the signature of sender's node (see Fig. 7). The authenticated nodes only can send RREP message to the source. Then, the authenticated nodes will be used for further data communication.

The data is securely transmitted to the corresponding receiver node when the protocol finds the secure and shortest path among the nodes (see Fig. 8).

The communication is performed among multiple nodes in NS2 environment; so many numbers of nodes are sharing the data at a time. It shows SOAR protocol increasing the performance of nodes in short time duration (see Fig. 9).

The simulation result of proposed SOAR routing protocol throughput comparisons in NS2 environment where the red colour defines Dynamic Source Routing (DSR) protocol throughput and the green colour defines the SOAR protocol throughput. The comparison takes time in X-axis, throughput in Y-axis. Within the

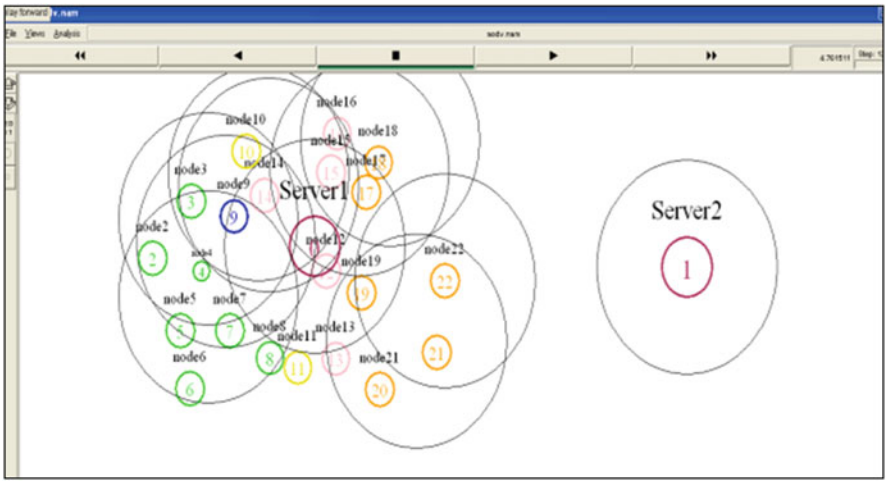

Fig. 7 Verification of digital signature

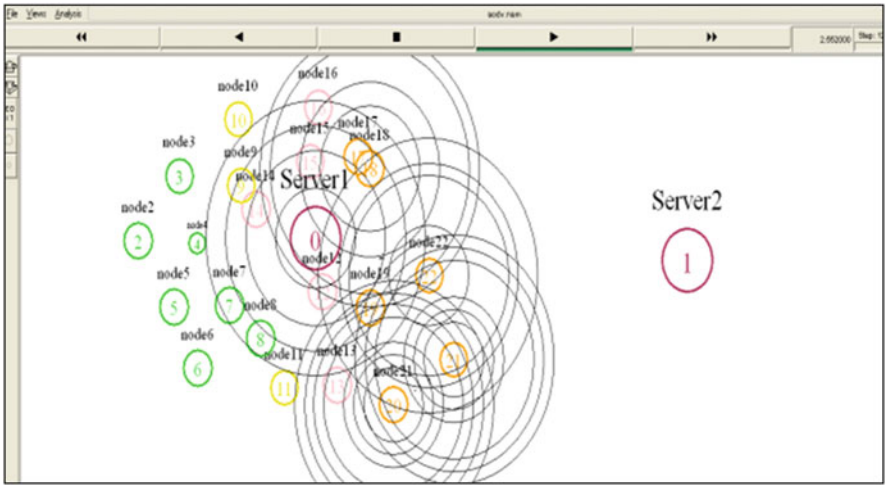

Fig. 8 Transmission of data packets

particular time period, SOAR protocol gives better result than DSR protocol (see Fig. 10).

The simulation result of packet delivery ratio in NS2 environment, where red colour means DSR protocol packet loss and green colour shows SOAR protocol packet loss. For comparing these two protocols, time is chosen for the X-axis and packetloss is chosen for Y-axis. Within the particular time period, the DSR protocol is suffered by a lot of packet loss, but in the SOAR protocol the packet loss is very less. So, SOAR protocol is better than the existing DSR protocol (see Fig. 11).

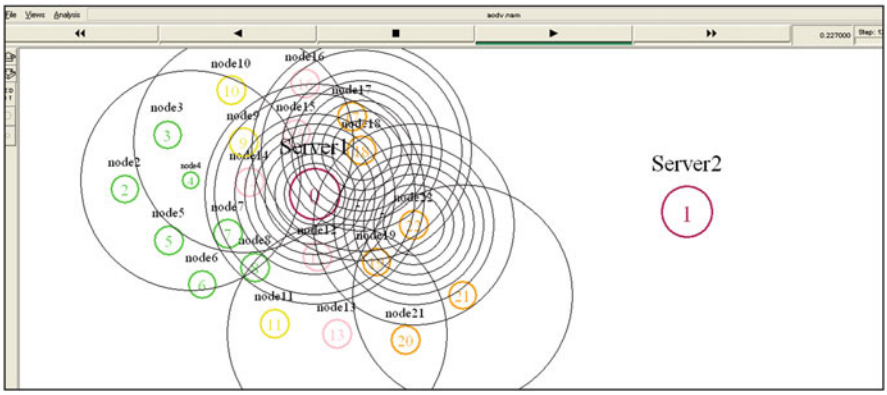

Fig. 9 Communication among multiple nodes

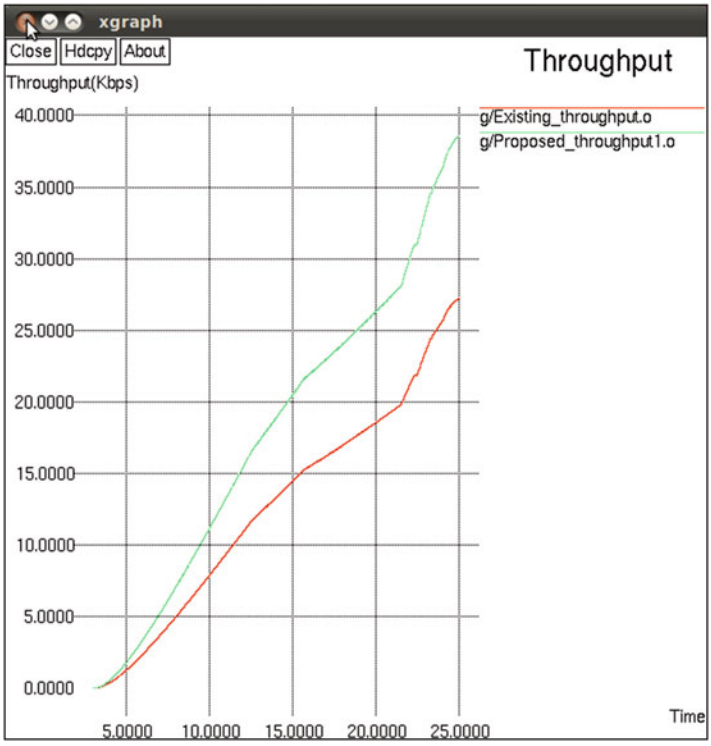

Fig. 10 Time vs throughput

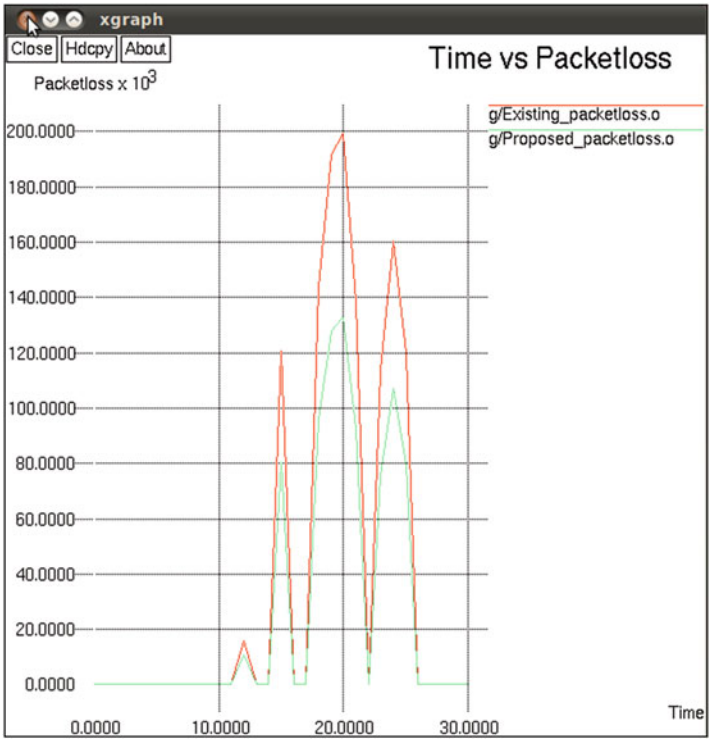

Fig. 11 Time vs packetloss

5 Conclusion

This chapter proposes a Secured On-demand Adaptive Routing (SOAR) protocol for efficient data communication among devices without human intervention. This protocol provides authenticated route request, route reply message and finds shortest secure path for communication among nodes. This protocol is suitable for tremendous networks and consumes less processing time. The NS2 simulation results show that SOAR protocol gives better throughput and minimum packet loss than the existing routing protocol.

References

1. Rahul, S. (1999). Routing in IoT networks using CupCarbon simulator. In *7th international conference on signal processing and integrated networks 2020* (2nd ed.).
2. Sathya, R. (2020). Designing the routing protocol with secured IoT devices and QOS over MANET using trust-based performance evaluation method. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-020-02358-4.

3. Ahmad, S., et al. (2020). Towards energy and performance aware geographic routing for IoT-enabled sensor networks. *Computers and Electrical Engineering, 85*, 106643.
4. Michele, S., et al. (2020). Distributed learning algorithms for optimal data routing in IoT networks. *IEEE Transactions on Signal and Information Processing Over Networks, 6*, 179–195.
5. Hammi, B., Zeadally, S., Labiod, H., Khatoun, R., Begriche, Y., & Khi, L. K. (2020). A secure multipath reactive protocol for routing in IoT and HANETS. *Adhoc Networks, 103*, 102118.
6. Sharma, K. P., & Sharma, T. P. (2019). Dynamic load tuning for energy-hole avoidance in Corona model for a wireless sensor networks. *International Journal of Sensor Networks, 30*(1), 56–68.
7. Kumar, V., & Kumar, A. (2019). Improved network lifetime and avoidance of uneven energy consumption using load factor. *Journal of Ambient Intelligence and Humanized Computing, 10*(4), 1425–1432.
8. Haseeb, K., Islam, N., Almorgen, A., & Din, I. U. (2019). Secret sharing-based energy-aware and multi hop routing protocol for IoT based WSAN. *IEEE Access, 7*, 79980–79988.
9. Thigale, S. B., Pandey, R. K., et al. (2019). Light weight novel trust based framework for IoT enabled wireless network communications. *Periodicals of Engineering and Natural Sciences, 7*(3), 1126–1137.
10. Gauya, D. (2019). *A novel dynamic reputation-based source routing protocol for mobile adhoc networks* (Vol. 77). New York: Springer.
11. Hammi, M. T., & Hammi, B. (2018). A Serhrouchni Bubbles of trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security, 78*, 126–142.
12. Hao, S. (2018). A stable and energy-efficient routing algorithm based on learning automata theory for MANET. *Journal of Communications and Networks, 3*(2), 52–66.
13. Hammi, B., & Fayad, A. (2017). IoT technologies for smart cities. *IET Networks, 7*(1), 1–13.
14. Chze, P. L. R., & Leong, K. S. (2014). A secure multi-hop routing for IoT communications: Internet of things. In *(WF-IoT), 2014 IEEE world forum on, IEEE* (pp. 428–432).
15. Raza, S., Voigt, T., et al. (2013). Lithe: Light weight secure coap for the IoT. *IEEE Sensors Journal, 13*(10), 3711–3720.
16. Marchang, N., & Datta, R. (2012). Light-weight trust-based routing protocols for mobile adhoc networks. *IET Information Security, 6*(2), 77–83.
17. Parul, et al. (2010). A comparative study for secure routing in MANET. *International Journal of Computer Applications, 4*(5), 0975–8887.
18. Punitha, V., & Mala, C. (2020). Traffic classification for connectionless services with incremental learning. *Computer Communications, 150*, 185–199.
19. Punitha, V., & Mala, C. (2020). Traffic classification in server farm using supervised learning techniques. *Neural Computing and Applications, 33*, 1279–1296.