Materials Today: Proceedings xxx (xxxx) xxx

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

An efficient biometric based authenticated geographic opportunistic routing for IoT applications using secure wireless sensor network

S. Menaga [a], J. Paruvathavardhini [a], S. Pragaspathy [b], R. Dhanapal [c], D. Jebakumar Immanuel [d]

[a] Electronics and Communication Engineering, Jai Shriram Engineering College, Tiruppur, India
[b] Department of Electrical and Electronics Engineering, Vishnu Institute of Technology, Bhimavaram, Andhra Pradesh, 534202, India
[c] Department of Computer Science and Engineering, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, 641021, India
[d] Department of Computer Science and Engineering, SNS College of Engineering, Coimbatore, Tamil Nadu, 641107, India

ARTICLE INFO

Article history:
Received 26 December 2020
Received in revised form 26 December 2020
Accepted 10 January 2021
Available online xxxx

Keywords:
Biometric authentication
BAGOR algorithm
Denial-of-Service attacks
Geographic opportunistic routing
Statistic state information

ABSTRACT

The applications of Wireless Sensor Networks (WSNs) are been broadly utilized in the field of Internet of Things (IoT) under communication framework. Notwithstanding services gave by the WSNs, numerous IoT-related applications necessitate reliable and secure delivery of data over unsteady remote connections. In-order to ensure secure and reliable delivery of data, many existing paper works accomplish authentication based routing algorithms with numerous forwarders within the Wireless Sensor Networks. Be that as it may; these types of approaches are vulnerable to genuine attacks like Denial of Service (DoS), where countless duplicate data packets are intentionally dispatched to destination node which disturbs the typical activities of wireless sensor networks. So, here we propose a new scheme of security algorithm for the wireless sensor networks. Our method, Biometric based-Authenticated Geographic Opportunistic Routing (BAGOR) algorithm depends on the user biometrics to shield the violation of DoS attacks, in order to meet out the validness requirements and reliability in the network. By examining biometric and statistic state information (SSI) of remote connections, BAGOR uses a trust model as statistic state information to get better proficiency of packet delivery. Dissimilar to past pioneering routing algorithm, BAGOR guarantees data honesty by building up an entropy-deployed selective validation algorithm and can detach DoS aggressors and reduce the computational expense. Thus, the eveloped procedure is assessed and compared with already existing security techniques. The simulations show that BAGOR decreasing system traffic, shielding against Denial of Service attacks, and expanding the lifetime of a sensor node in the network. Thus, the usefulness and execution of the whole system is enhanced.

Selection and peer-review under responsibility of the scientific committee of the Emerging Trends in Materials Science, Technology and Engineering.

1. Introduction

Wireless sensor networks (WSN) is a group of spatially spaced sensor nodes in different fields under different environmental conditions collecting data and sending it to the sink node for further processing. The further processing here refers to the accumulation of data according to the required or the specified conditions and sending it to the processor. This sending part (i.e.) data transmission is the significant part that is to be considered now because an appropriate routing protocol should be used to achieve the maximum throughput with minimum delay and attacks. In recent days, the WSNs are used along with IoT (Internet of Things) in various applications like healthcare, surveillance, smart grids, industries, physical and environmental condition monitoring etc. Fig. 4.1 Fig. 4.2.

So a reliable and efficient data delivery is substantially important in these kind of applications, as the data has to travel in multiple paths from the time of collection, accumulation, processing, cloud storage, again to the receiver who has to deal with it.

Sometimes the WSNs are vulnerable to link failures caused by the interference, signal fading, redundant data, reduced QOS [1,2], therefore an efficient approach in transmitting and defending the data from DOS attacks is a challenging issue in WSN which lead to reduce in the quality of service. Many different approaches were developed in order to meet out this requirement which temporar-

E-mail address: dhanapal.r@kahedu.edu.in (R. Dhanapal)

https://doi.org/10.1016/j.matpr.2021.01.241
2214-7853/
Selection and peer-review under responsibility of the scientific committee of the Emerging Trends in Materials Science, Technology and Engineering.

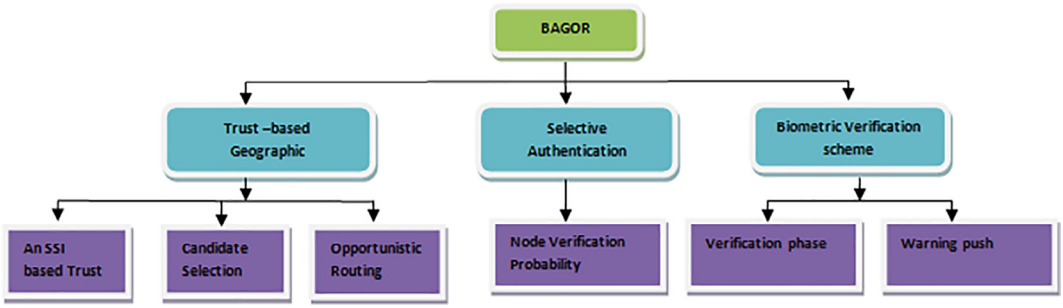

Fig 4.1. Overview of BAGOR.

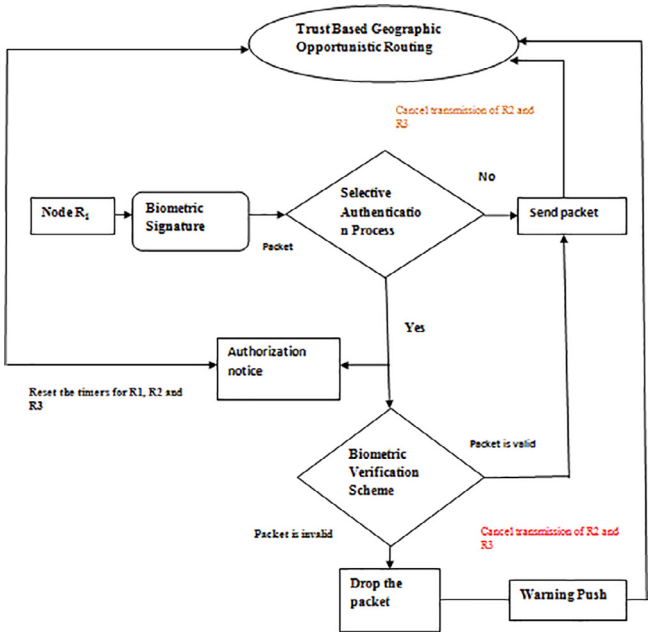

Fig 4.2. The working flow diagram of BAGOR.

ily solved the issue. As the technology is getting updated, many new issues are also developed.

Currently an efficient algorithm to attain the reliable packet delivery is accomplished by geographic opportunistic routing (GOR). The geographic routing doesn't require any maintenance or route establishment and it uses the position or location of the nodes to transmit a data [3,4–7].In opportunistic routing instead of transmitting the data by single forwarder, sender node selects multiple candidates to forward the data.

Thus the data transmission will not be interrupted until a single candidate node in the set of forwarders, relaying the packet effectively. The geographic opportunistic routing is found to have an improved performance than multipath routing, as no signal interference exists between candidates.

Thus, the fusion of opportunistic routing and geographic routing is called as geographic opportunistic routing (GOR) [8-10]. Already existing (GOR) geographic opportunistic routing methodologies can attain high level of reliable data delivery over remote connections (e.g., [10]). Yet, they experience the ill effects of genuine attacks like Denial of Service. Malicious nodes might intentionally transfer a huge number of invalid packets with unauthorized signatures to sink node, in order to squander the resources of the network and disturb the typical activities of wireless sensor networks [11]. Specifically, opportunistic routing infuriate Denial of Service attacks, that invalid information could be dependably delivered to recipients with many candidate node forwarders, that will be approved by the hypothetical examination. We need a security verification conspire to guard against these attacks, such that it can ensure the data packets are transferred from real nodes, and they are not procured or modified by aggressors in the time of transmissions. Be that as it may, this opens a lot of new issues. Initially, including a current digital signature plot for validation may massively expand the computational rate of a node in the network and broaden the deferral of packet delivery.

In this paper, we offer an equipped client verification method for the applications of wireless sensor network. This plan survives the validation issue and enhances the effectiveness of wireless sensor network. We develop a verification conspire called as Biometric based-Authenticated Geographic Opportunistic Routing (BAGOR) algorithm. The motivations behind the structured authentication mechanisms are as per the following:

(i) Increase the performance of the network by decreasing system traffic.

(ii) Spare the battery intensity of the sensor nodes, hence improving the lifetime of the wireless sensor network; and

(iii) Safeguard the node against various kinds of malicious node attacks, in this way enhancing the execution and system performance.

A proposed lightweight authentication (BAGOR) algorithm to disconnect DoS aggressors in WSNs. Second, the opportunistic routing will define the need of candidate forwarders through separate verification of data packets, since the authentication delay is commonly a lot more noteworthy than the transmission period of data packets. Consequently, re-establishing the priorities of candidate node forwarders to accomplish the reliability and integrity of information ought to be our principle structure objective. Third, the opportunistic routing will bring out the copy transmission of invalid information or repetitive verification. Our BAGOR could square 85% of invalid information with a less number of communication overhead, at the same time as it spares half of the computational resources in the network and half 70% of data transmission rate contrasted with different plans.

2. Related work

There are several works proposed in-order to overcome the different kinds of DOS attacks using geographic and opportunistic routing separately, now these two techniques are combined which is called as GOR [12–15]. Venkatesh et al., [16] have proposed a geographic and opportunistic routing algorithm based on two hop information using path reliability and best energy strategy, the algorithm identifies the degree radian area (DRA) and selects the node within that area by checking whether the angle of inclination is $\theta/2$. A flag bit is added to the data to check whether it is received by the user, then again from there the second node is selected using the same procedure. Long cheng et al., [17] has

developed an efficient quality of service (QoS) aware geographic opportunistic routing (GOR) which is used to improve the provisioning of QoS, to achieve end-to-end efficiency and latency via multihop transmission of data. Abdul Mateen et al., [18] has proposed GEDPAR and E2EVHR protocol to eliminate the void hole problem (an area where transmission is not possible) and to improve the transmission efficiency and network power efficiency. Chen Lyu, et al., [19] has proposed a SelGOR(Selective authentication based geographic opportunistic routing) routing algorithm in which unnecessary transmission of packets is controlled by opportunistic routing and the proper location is chosen to send the data using the geographic routing. Along with this a digital signature is added to authenticate the user.

Patil.A.C, et al [20], has proposed a prevention technique called Co-FAIS which acts as an immune system to the WSN and it uses fuzzy logic. It has six different modules like 1. Sniffer module, 2. Fuzzy misuse detector module, 3.danger detector module, 4.Fuzzy Q-learning Vaccination Module, 5. Cooperative Decision Making Module, 6.Response Module.Ademola P. Abidoye,etal, [21] has proposed a method for detection and countermeasures for attacks of DDOS(Distributed denial of service), in which Diffie–Hellman key exchange algorithm is used which helps the base station to generate new symmetric secret keys and distributes to all the SNs. Then message integrity ensures that the data packets received at the received node is not corrupted by computing the hash function for the message received and then decrypting using the copy of the shared secret keys. SU Maheswari,et al, [22] has proposed a method that fights against the DOS attack particularly(Hello flood attack), in this method a new protocol called Robust formally analyzed routing protocol for wireless sensor network deployment (RAEED) is been used in which bi-directional verification scheme is used. Messages will send a ASK message and will be waiting for the ASSIGN message to share the data. Only the nodes having bi-directional link can send the ASSIGN message so the malicious nodes are easily avoided here.

Rolla.p,et al,[23], has proposed a forward window technique in which dynamic time can be set for requesting a node. Here, the source node in the first half communication will send route request to the nodes in the second half. The malicious nodes present in the first will also send numerous number of requests, but the nodes can identify and reject those messages using dynamic time in forward window technique.

Althobaiti, O, et al,[24], has proposed an efficient biometric authentication routing protocol for the WSNs by using the iris as the biometric authenticity to regenerate the user's key every time on the fly. This a secured way of protecting the data from unauthorized users and the key used in this protocol is stronger than the password but also shorter than the biometric data. Wang, F.,et al, [25] has proposed an advanced biometric based authentication scheme using Chebychev chaotic map to prevent the WSN by not disclosing the session key. It helps to prevent the imitation attack, desynchronization attack, important session information attack. Yu.S, et al,[26] has proposed a new protocol with three phases namely1.User registration phase 2. Sensor node registration phase 3.Authentication phase. This ensures the WSN from impersonation attack, session key disclosure attack, replay attack, smart card stolen attack, anonymity and mutual authentication.

3. Network and security model

Here, we expect a multi-hop WSN which comprises various sensor nodes and a few sinks, and is conveyed for the utilization of internet of things. The sensor nodes inside the remote transmission range can straightforwardly transmit information between one another.

This multi-hop correspondence is empowered if their Euclidian separation is more prominent than the range of transmission. We presume that the sensors arranged are a dense system, every node has a lot of neighbor hubs (nodes). Consider that the sensor nodes are fixed, and sense their area data and the location of sink nodes. Plus, in geographic routing every nodes know about the area data of their nearby nodes by the beacon messages, i.e., a node intermittently communicates beacon messages which consists of its identity, area data and lingering energy [27].

As the battery issue is a significant test in the wireless sensor network, we accept that sinks are furnished with incredible gadgets and the remaining nodes work on restricted energy of the battery. A node can get the energy data of their nearby nodes by viewing the beacon messages.

Here in our work, we fundamentally focus on the exhibition of secure packet conveyance in the network layer. In-order to accomplish the coordination of candidate node forwarders in the algorithm, and a modified medium access control (MAC) protocol that is developed for opportunistic routing dependent on RTS/CTS/ACK component in the IEEE 802.11b [9].

On the off chance that a malicious node catches a message switched between an authorized user node and a sensor node and it will try to get mystery network data. For ensuring security, the key management in WSN using Public Key Infrastructure (PKI) [28]. Consider each node in the network has two keys such as private key for signing data packets and a public key for the verification process by the process of biometric signing schemes [29].

The goal of our protocol is to design a secured and reliable packet transmission from sender to destination node for which the following important properties have to be considered for each data packet:

3.1. Data integrity

Prior to sending a packet, a sensor node should guarantee the validness of data transferred by its nearby nodes. Something else, base node (sink) would get a lot of invalid packet from the Denial of Service attackers, that disturbs the ordinary tasks of utilizations. To give the property of data packet integrity, a validation conspire is imperative for wireless sensor networks. This administration gives confirmation that imparted information can't be modified by the unapproved node. With BAGOR's, the data packet integrity is given utilizing a single one-way hash function, which is a data packet transmitted by the user node to the trust node. So also, all imparted messages aresent similarly, which can't be changed by anmalicious node.

3.2. Data reliability

Due to the transmission and shared mechanism of the remote link, data packets are vulnerable to lose when the connection fails. Indeed, the impact of packet loss is unavoidable in wireless sensor networks; it shouldn't stop the tasks of applications dependent on Internet of Things. Hence, it is basic to ensure highly reliable for any packet delivery protocol.

3.3. Non-Repudiation

The non-repudiation normally includes authentication. It allows a sink node to demonstrate to the outsider nodes which is answerable for the data packet. A sink node can identify invalid data packets sent by the sender and also report about attackers to a trusted node.

3.4. Denial of service attacks resistant

With no confirmation scheme, the denial of service attackers may transmit a great deal of duplicate packets inside the network to squander correspondence networks resources or upset the typical packet delivery. Also, capability of sensor nodes ordinarily have restricted computational and battery resources. For protecting the nodes from denial of service attackers, the verification plan should have low computational rate for providing energy efficiency in wireless sensor networks.

When a user joins the wireless sensor network, BAGOR algorithm utilizes fingerprints to authenticate them in order to provide security insurance. Also, this biometric fingerprint verification technique doesn't need any extra hardware. Without much of a stretch, the biometric data can easily be availed from their personnel device, for example, a mobile or computer. To get data from a node in the network, client can transmit message to sensor node straightforwardly that would be in the scope of the query device. So as to inquire a node, client might utilize any electronic device with a biometric fingerprint sensor, i.e., smart phone, note pad, PDA and so forth. Numerous users are permitted to get to wireless sensor arrange through their personnel smart phones. Before the arrangement of network, all nodes are preinstalled with mystery data. Because of the mystery data, believed node verifies sensor node which is engaging the client request. The proposed BAGOR algorithm uses a WSN with Mica2 sensor nodes and base station (trust node-TN) which goes about as authenticator of both the client and the sensor nodes. Trust node is dependable and secure with predominant resources as far as data storage, computation and battery.

4. Routing and authentiction methodology

4.1. Biometric based Authenticated geographic opportunistic routing

The routing and authentication of BAGOR algorithm comprises with three primary components as: Trust based Geographic routing algorithm, selective authentication algorithm and biometric verification schemes.

4.2. Trust-based geographic opportunistic routing

A sensor node sets up a SSI-based trust model and progressively refreshes it in WSNs by collecting and examining historical data transmission of remote connections. Once the data packet is received at the sensor node, immediately the candidate node will be selected by the node based on forwarder set from its next hop nodes so as to accomplish trustworthy data conveyance in opportunistic routing. In-order to achieve this, the sensor node allocates the priority to every applicant forwarder dependent on the routing metric that is characterized on the trust model. Along these lines, trust-based geographic opportunistic routing incorporates a SSI-based trust model, candidate selection and opportunistic routing.

4.2.1. Statistic state information (SSI) -Based trust model

On gathering and examining complete data packet transmission of nearby (neighbor) nodes, we determine the ratio of the quantity of data packets effectively conveyed to the quantity of data packets transmitted to characterize the trust of a connection. During the period of significant level, a k^{th} node separates the total time into a continuous sequence of intervals, which will have a similar size n. At every observation intervals, it is feasible for the node k to listen the remote link furthermore, monitor whether the packet is really sent by the chosen neighbor sensor node. The quantity of data packets sent for a one interval by the neighbor node j referred as $NS_{jk}(n)$ the quantity of data packets sent to it is mentioned as $ND_{jk}(n)$. Hence the sensor node k can estimate the trust of the connection $C_{k,j,}$ which is given as $T_{ik}(n)$ $(0 \leq T_{ik}(n) \leq 1)$.

$$T_{ik}(n) = NS_{jk}(n) \;/\; ND_{jk}(n) \tag{1}$$

At the initial stage of a observation time interval, $NS_{jk}(n)$ is set to zero and $ND_{jk}(n)$ is set as one. When a sensor node (k) is relayed a data packet to sensor node (j) (next hop node) $ND_{jk}(n)$ is modified to $\alpha ND_{jk}(n) + 1$, in this $\alpha(0 \leq \alpha \geq 1)$ indicates the correction factor rate in the network. When k^{th} node comes to know a successful packet transmission by node j, $NS_{jk}(n)$ is increment by 1, so that the trust of the link connection $C_{k,j}$ is changed accordingly. The trust degree will change to negative if the transmission is failed [19].

The connection trust of $C_{k,j}$ at the time the of t is refreshed through emphases in k's node which is a nearby node in the neighbor list, this process helped to accomplish the dependability of the trust candidate node chosen in opportunistic routing,

$$T_{ik}(t) = \omega\, T_{ik}(t-n) + (1-\omega)\, T_{ik}(n) \tag{2}$$

Here ω refers the weight which can adjust the inclination among present and complete previous state data. If vagueness is not there as for the time, we use T_{ik} for brevity.

$$SH_{jk} = D(k,s) - D(j,s)$$

4.2.2. Candidate selection

Candidate selection is optimized in this routing based on the SSI-based trust model. From this SSI model, the sending k^{th} node can get the trust link $C_{k,\,j}$ from the neighbor list. Some links may become expired as the energy level of sensor nodes reduces. In the WSN, by the technique of cyclic beacon messages the k^{th} node have an awareness of node j energy. Suppose the node k need to transmit the data packet to sink, if node j is the next hop which is near to sink node, the single hop distance is evaluated by Euclidian distance among the k^{th} and j^{th} sensor nodes, a single node hop distance progress is defined as $SH_{jk:}$

Here the Euclidian distance, D (k,s) is measured between the k^{th} sensor node and sink node(s). The list of candidate node forwarder set for sensor node (k). is given by (Q_k) based on the value of routing metric. The candidate node in the list are arranged in the drop down order.

4.2.3. Opportunistic routing

Following the selection of candidate, the sender/middle node k is prepared to transmit a packet to the sink node. The selective authentication algorithm is initially played out to give preference to verify the packet or not. At the point of avoiding the verification measure or the check result is valid, then the data packets are broadcast, which incorporates the candidate lists and their priorities as per routing metric. In this type of routing, based upon the allocated priority every forwarder node directs the data packet.

A timer time (j) τ, order (j) is initiated by the candidate node j when the data packet is received correctly. Here a constant is defined by τ and the priority of the packet is denoted by order (j). Accordingly, minimum timer value will be assigned to the highest priority node. Then the initial candidate node itself will act as the next-hop sender. That node will build up own forwarder node list, and plan for the further packet transmission.

As per the timer, the other less-priority candidate sensor node reserves the received information packet and it waits for next packet transmission to begin. In the event that it listens that the packet is been communicated by some other high-priority node, it will drop the packet and the timer. If the timer terminates, the candidate node ready to act as the next-hop sender, and also initi-

ates to transmit the data packet. The same procedure is continued until it reaches the sink node successfully.

4.3. Selective authentication algorithm

We need security feature in order to improve the trust in exchanging the information over the in secured network. So we can create private and public key pair for authenticating the users to access the data. There will be a pair of public keys in which one will be used to encrypt and the other to decrypt, usually the public keys will be used attached with the digital certificates which will be publicly available so the intermediate users can use that key to access the data. The private keys can be protected by the user with a personal password, as the pc or smart phone can be easily hacked we use a new method to generate this private key password by using the biometric feature of the users like iris recognition, finger print, face recognition etc. This biometric key is generated with the help of biometric template and this has to very precise so as to create the same private key each time.

In a communication, the data packet has to travel throughout the network, sometimes there will be bogus data packets from the malicious nodes resembling the original data packets. This is actually done to overload the traffic in the network so that it affects the normal communication which results in denial of service for other data packets. Therefore to identify duplicate packets, the original data packets involving in the communication should be assigned with a private key and a public key, biometric authentication by the user is used as a private key here. Checking of all the data packets for the authentication by all the nodes at all times is time consuming which results in data delivery delay, so we preferably check the packets with low probability in our algorithm. The information about the neighboring nodes should be known to fix the probability dynamically depending on the received invalid data packets. Let $V_{(x,y)}$ (where $\times$ &y are the nodes involved in the communication) be the probability, which is set to 0 for benign nodes ($V_{(x,y)}$ -> 0) and is set to 1 for malicious nodes ($V_{(x,y)}$ -> 1). This probability value is assigned to all the nodes in such a way that it checks for low probability in all the data packets received by any of its neighboring nodes and isolates the attackers. Therefore this selective authentication algorithm will verify the first data packet from the new neighboring node and sets a ($V_{(x,y)}$ -> 0) for the latter data packets from that node confirming that is not a duplicate node and then this malicious nodes that was disturbing the communication will be totally blocked from the communication.

4.4. Biometric verification scheme

The verification conspire is proposed to optimally incorporate a specific confirmation calculation into a trust-based geographic opportunistic routing. When the node chooses to check an information packet at this point, the node separates the priorities of competitor forwarder nodes characterized through the opportunistic routing method. This is on the grounds that the checking time of a signature is a lot more noteworthy than the transmission time [30]. In this way, we plan the process of confirmation notice inorder to reestablish the priorities of forwarder nodes in routing. Once confirmed, the warning push system is used to confer the checked data of void marks among the candidate nodes for effectiveness. This empowers BAGOR to quicken the detachment of DoS attackers, and evade copy void data transmission or excess signature confirmation.

4.5. Verification phase

If a source or a forwarder node initiates data transmission, it broadcasts the verification notice packet. A verification notice consists of its sender identity and the sequence number of the packet, verification time estimation and identities of low candidate nodes.

Once the notice of verification is received, a candidate node indicated in data packet increments the timer according to the verification time. Then the signature is validated by higher priority sensor node in order to authenticate low priorities node which is in waiting for transmission. By resetting the timers, candidate nodes are rearranged with respect to the priorities.

4.6. Warning push

A relay node forwards the data packets once the signature matches with the public key of the sender node, in case of mismatch the data packets are considered as invalid and the forwarder node drops the packet. If the signature is recognized as invalid, the forwarder fine tunes the verification probability of its previous forwarder node. As delineated in Fig. 4.3, the relay node R2 increment the verification probability of node A, if M is not valid. Additionally, a warning push packet that has the identity of forwarder node, identity of previous relay node, the information packet's identifier and identities of the less priority candidate nodes which is communicated by the relay node.

After getting the warning push, a candidate's node indicated in the data packet executes two tasks. From one perspective, the candidate node increments the previous node's verification probability. In our model, node R2 and R3 increment the verification probability of node A, when they get a warning push packet from node R1. Then again, the packet will be dropped by the candidate node and it also stops its timer. By the shared verification information among neighbors in the network, other candidates know about void packet. At last, they straightforwardly end the transmission process and without extra verification it decides to drop the packet, which essentially lessens the expense of bandwidth resources.

5. Results and discussion

5.1. Performance Evaluation

By using NS2 software, eighty nodes have been created to show the simulation of defense of attacks and to analyze the performance of BAGOR algorithm under the DOS attack as shown in Fig. 5.1. Here the improved reliability of BAGOR is proved by comparing with three other routing algorithms using different link qualities. The wireless link quality is assorted from the value of 0

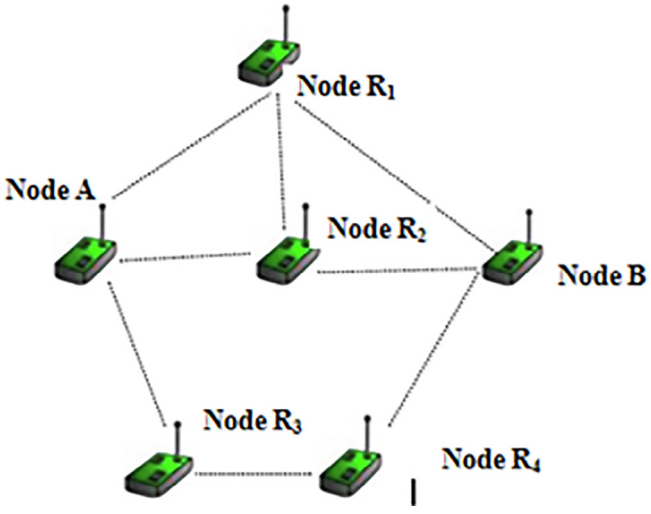

Fig 4.3. Network topology.

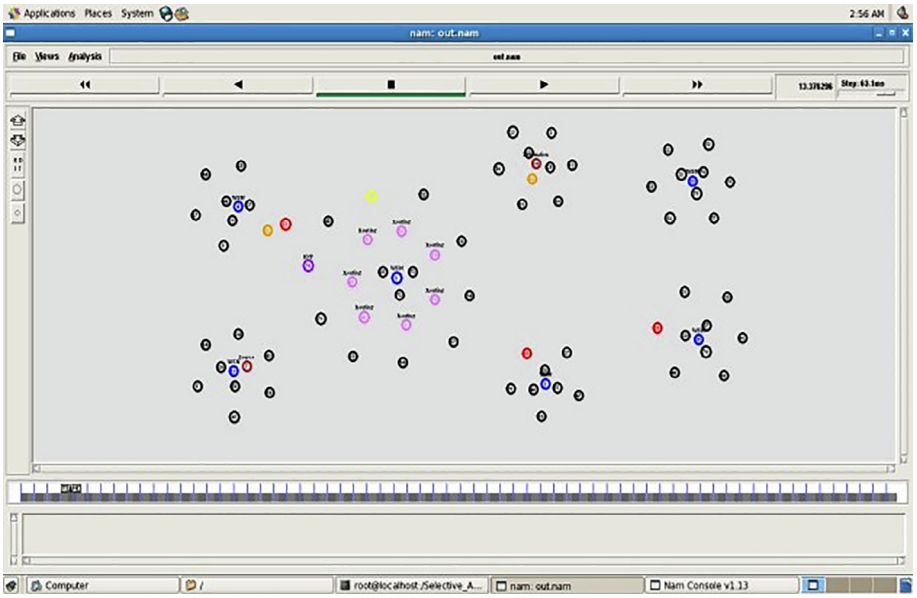

Fig 5.1. The simulation window which shows the node creation.

to 8 for the test analysis. Biometric based key pairs are used by the sensor nodes for authentication process of the packet which is in size of 512bytes and the number of forward candidates are 2 in number.

5.2. Transmission overhead of void packets

It is the average number of void packets that has been sent by the malicious nodes in the network [19]. Fig. 5.2 shows the transmission overhead of invalid packets with respect to various qualities of link. From the analysis, it has been indicated that the BAGOR has the most minimal transmission overhead, and significantly protects the node computational resources. By the implementation of different candidate node forwarders, GPSR has doubled the rate of transmission overhead than the EQGOR, which tentatively affirms that the denial of service attacks are severe for opportunistic routing.

5.3. Control packet Overhead

It can be measured as the quantity of additional packets for information conveyance per unit time (no. of bits per second), it also includes beacon packets, warning push and the verification notice messages [19]. Fig. 5.3 shows the plots of the control packet overhead under various connection characteristics. From the graph it is very clear that BAGOR algorithm is able to control the packet overhead than the other algorithms as we use biometric authentication scheme and warning push.

5.4. Data packet delivery Ratio

It can be defined as the ratio of the number of data packets got at the sinks to the quantity of data packets sent by the sender node [19]. Fig. 5.4 delineates the data packet delivery ratio under various link qualities. If the connection quality reductions, numerous data

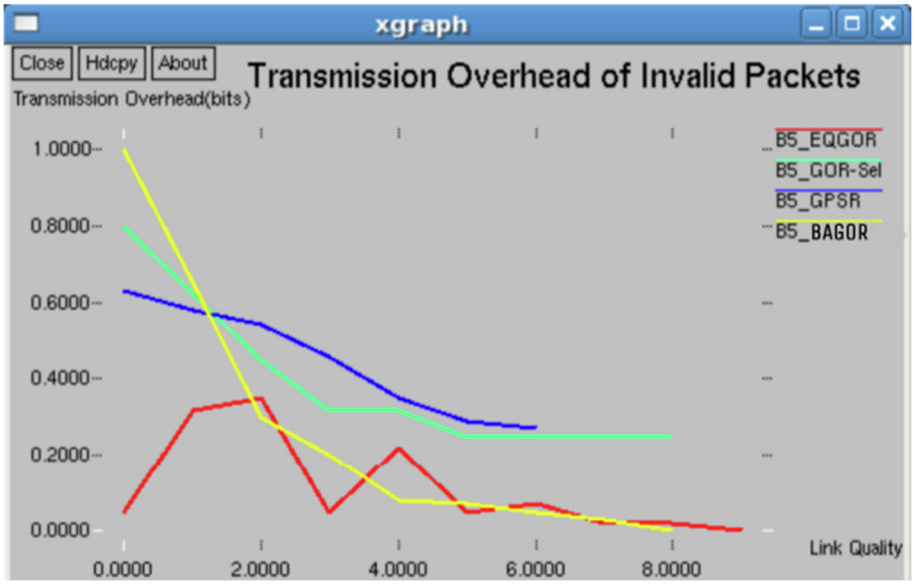

Fig 5.2. Transmission overhead of invalid packets.

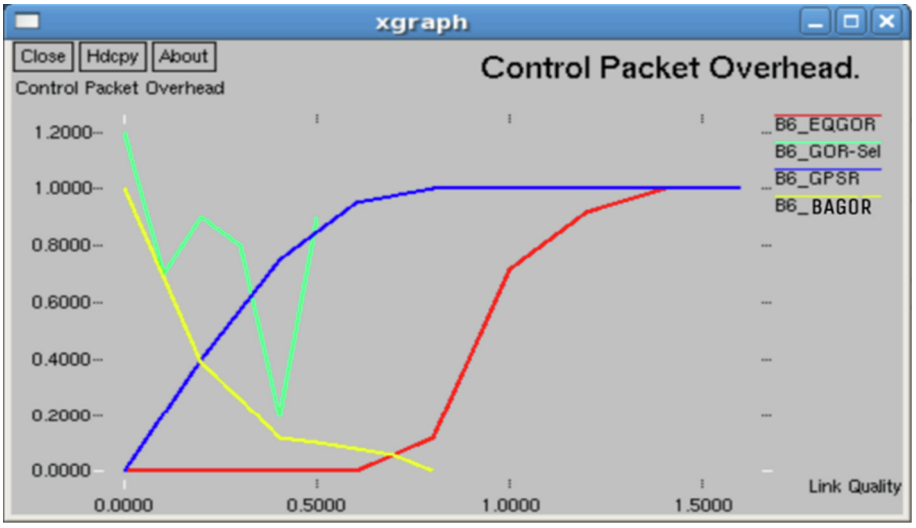

Fig 5.3. The control packet overhead is best controlled by BAGOR algorithm.

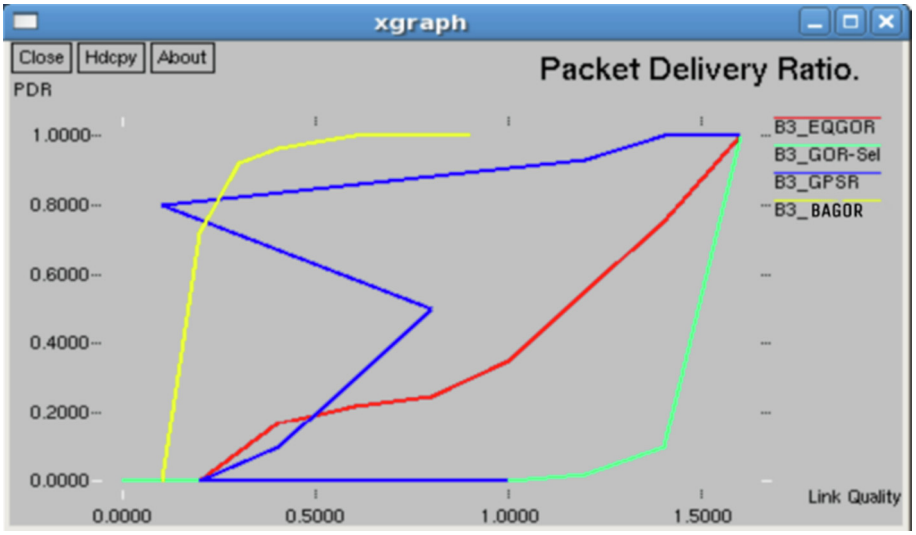

Fig 5.4. The improved packet delivery ratio.

packets are dropped on the way of the path and the packet delivery ratio of the apparent multitude of plans decay. The Fig. 5.4 demonstrates that BAGOR perform better than EQGOR, GOR-Sel, GPSR algorithm which shows that coordinating our statistic state information model into the steering metric could viably advance the reliability of data transmission.

5.5. End-to- end packet delay

It is the normal time for the information packets transmitted from source nodes to sinks, including both the substantial and invalid information packets (seconds)[19]. Fig. 5.5 demonstrates performance of end-to-end packet delay under various qualities of link. The authentication in network unavoidably increases the delay of packet delivery. Due to the poor link quality, more number of packets are lost, it is indicated that the delay of GPSR and EQGOR pointedly increased. This is on the grounds that repetitive verification have been caused by opportunistic routing. By the plan of warning push messages, BAGOR algorithm could decrease the quantity of verification and the delay execution isn't influenced much by the link quality.

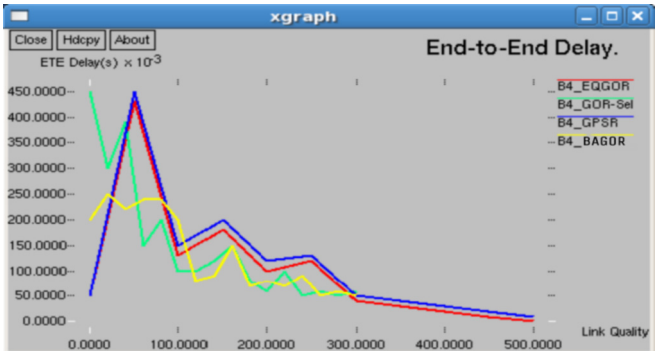

Fig 5.5. The end-to-end delay.

Thus the proposed BAGOR algorithm is proved to perform better than the other algorithms in preventing nearly 85% of the invalid data packets. It is very efficient in dropping the invalid packets in first two hops by using the co-operative verification scheme. It therefore, reduces the transmission overhead packets which minimizes the total traffic in the network.

6. Conclusion

In this paper, we have derived an efficient BAGOR algorithm to provide a secured WSN by using biometric authentication and reliable data transmission for IOT based applications. The BAGOR algorithm is a biometric based geographic opportunistic routing, which completely makes use of the Statistic State Information model could improve the data packets reliability. Biometric authentication is used to defend against the Denial of Service (DoS) attacks caused by malicious nodes or sometimes due to the opportunistic routing. This seems to be a light weight algorithm in which energy is not consumed much and also with low computational cost when compared to the other algorithms. Along with the biometric authentication algorithm, we use the co-operative selection algorithm to reduce the repeated checking and directly drop the unwanted or unauthenticated packets.

Our simulation results very clearly proves that the BAGOR algorithm works effectively in blocking the invalid data packets by following the different steps defined in the algorithm. However end-to-end delay seems to be little long because of the verification process. We plan to study about this delay process and articulate a method of improving this end-to-end packet delay in our future work. Furthermore, different types of biometric authentication may be tried in the work like iris authentication whose error seems to be very less.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Comput. Netw. 54 (15) (2010) 2787–2805.
[2] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things(IoT): A vision, architectural elements, and future directions, Future Gener Comput. Syst. 29 (7) (2013) 1645–1660.
[3] [3] L. D. Xu, W. He, and S. Li, Internet of Things in industries: A survey, IEEE Trans. Ind. Informat., vol. 10, no. 4, pp. 2233_2243, Nov. 2014.
[4] [4] G. Schaefer, F. Ingelrest, and M. Vetterli, Potentials of opportunistic routing in energy-constrained wireless sensor networks, in Proc. 6th Eur.Conf. Wireless Sensor Netw., Cork, Ireland, Feb. 2009, pp. 118_133.
[5] R. Sanchez-Iborra, M. Cano, JOKER A novel opportunistic routing protocol, IEEE J. Sel. Areas Commun. 34 (5) (2016) 1690–1703.
[6] J. Luo, J. Hu, D.Wu, and R. Li, Opportunistic routing algorithm for relay node selection in wireless sensor networks, IEEE Trans. Ind. Informat., vol. 11, no. 1, pp. 112_121, Feb. 2015.
[7] J. So and H. Byun, Load-balanced opportunistic routing for duty-cycled wireless sensor networks, IEEE Trans. Mobile Comput., vol. 16, no. 7, pp. 1940_1955, Jul. 2017.
[8] K. Zeng, Z. Yang, and W. Lou, Location-aided opportunistic forwarding in multirate and multihop wireless networks, IEEE Trans. Veh. Technol.,vol. 58, no. 6, pp. 3032_3040, Jul. 2009.
[9] S. Yang, C. K. Yeo, and B. S. Lee, Towards reliable data delivery for highly dynamic mobile ad hoc networks, IEEE Trans. Mobile Comput., vol. 11, no. 1, pp. 111_124, Jan. 2012.
[10] L. Cheng, J. Niu, J. Cao, S. K. Das, and Y. Gu, QoS aware geographic opportunistic routing in wireless sensor networks, IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1864_1875, Jul. 2014.
[11] D. R. Raymond and S. F. Midkiff, Denial-of-service in wireless sensor networks: Attacks and defenses, IEEE Pervasive Comput., vol. 7, no. 1, pp. 74_81, Jan./Mar. 2008.
[12] G. Schaefer, F. Ingelrest, and M. Vetterli, Potentials of opportunistic routing in energy-constrained wireless sensor networks, in Proc. 6th Eur. Conf. Wireless Sensor Netw., Cork, Ireland, Feb. 2009, pp. 118_133.
[13] R. Sanchez-Iborra, M. Cano, JOKER A novel opportunistic routing protocol,", IEEE J. Sel. Areas Commun. 34 (5) (2016) 1690–1703.
[14] [14] J. Luo, J. Hu, D.Wu, and R. Li, Opportunistic routing algorithm for relay node selection in wireless sensor networks, IEEE Trans. Ind. Informat., vol. 11, no. 1, pp. 112_121, Feb. 2015.
[15] J. So and H. Byun, Load-balanced opportunistic routing for duty-cycled wireless sensor networks, IEEE Trans. Mobile Comput., vol. 16, no. 7, pp. 1940_1955, Jul. 2017.
[16] Venkatesh, Achar, L.A., Kushal, P. and Venugopal, K.R., 2019. Geographic opportunistic routing protocol based on two-hop information for wireless sensor networks. International Journal of Communication Networks and Distributed Systems, 23(1), pp.93-116.
[17] L. Cheng, J. Niu, J. Cao, S.K. Das, Y. Gu, QoS aware geographic opportunistic routing in wireless sensor networks, IEEE Trans. Paral. Distrib. Syst. 25 (7) (2013) 1864–1875.
[18] A. Mateen, M. Awais, N. Javaid, F. Ishmanov, M.K. Afzal, S. Kazmi, Geographic and opportunistic recovery with depth and power transmission adjustment for energy-efficiency and void hole alleviation in UWSNs, Sens. 19 (3) (2019) 709.
[19] C. Lyu, X. Zhang, Z. Liu, C.H. Chi, Selective authentication based geographic opportunistic routing in wireless sensor networks for Internet of Things against DoS attacks, IEEE Access 7 (2019) 31068–31082.
[20] S. Patil, S. Chaudhari, DoS attack prevention technique in Wireless Sensor Networks, Procedia Comput. Sci. 79 (2016) 715–721.
[21] A.P. Abidoye, I.C. Obagbuwa, DDoS attacks in WSNs: detection and countermeasures, IET Wireless Sens. Syst. 8 (2) (2017) 52–59.
[22] S.U. Maheswari, N.S. Usha, E.M. Anita, K.R. Devi, in: A novel robust routing protocol RAEED to avoid DoS attacks in WSN, IEEE, 2016, pp. 1–5.
[23] P. Rolla, M. Kaur, in: Dynamic forwarding window technique against DoS attack in WSN, IEEE, 2016, pp. 212–216.
[24] O. Althobaiti, M. Al-Rodhaan, A. Al-Dhelaan, An efficient biometric authentication protocol for wireless sensor networks, Int. J. Distrib. Sens. Netw. 9 (5) (2013).
[25] F. Wang, G. Xu, G. Xu, A provably secure anonymous biometrics-based authentication scheme for wireless sensor networks using chaotic map, IEEE Access 7 (2019) 101596–101608.
[26] S. Yu, J. YoungLee, M. Kim, Y. Park, in: A Secure Biometric Based User Authentication Protocol in Wireless Sensor Networks, IEEE, 2020, pp. 0830–0834.
[27] [27] B. Karp and H. T. Kung, GPSR: Greedy perimeter stateless routing for wireless networks, in Proc. Annu. Int. Conf. Mobile Comput. Netw.(MobiCom), Boston, MA, USA, Aug. 2000, pp. 243_254.
[28] A. Perrig, J. Stankovic, D. Wagner, Security in wireless sensor networks, Commun. ACM 47 (6) (2004) 53–57.
[29] S. Mohammadi, S. Abedi, in: ECC-based biometric signature: A new approach in electronic banking security, IEEE, 2008, pp. 763–766.
[30] P. Ning, A. Liu, W. Du, Mitigating DoS attacks against broadcast authentication in wireless sensor networks, ACM Trans. Sensor Netw. 4 (1) (2008) 1–35.