SelGOR in Wireless Sensor Networks for IoT against Daniel of Service (DoS) attacks

Goutham V[1], Lakshmi D L[2]

[1,2]*Assistant Professor, Dept. of ECE, BGS Institute of Technology, BG Nagara, Mandya District, Karnataka, India*

Abstract - *Communication system for IoT is Wireless Sensor Networks (WSNs) which requires data transfer to be reliable over the wireless links which are unstable. In the present works on GOR, to guarantee the data delivery reliable, multiple forwarder candidates are used in the sensor networks which suffers from the attacks of denial of service, which delivers the huge number of invalid data to the receiver which breaks the normal operation of sensors networks. Here it is proposed a new routing technique i.e. SelGOR which defends the DoS attacks which provides authenticity and reliability in the sensors networks, which also reduce the cost of computation. It also influences the trusted models based on SSI which improves the data delivery. A new scheme is designed which isolates the attackers i.e. DCV (distributive co-operative verification).*

***Key Words*: Selective Authentication, GOR: Geographic Opportunistic Routing, opportunistic routing, DoS attacks, Wireless Sensor Network**

1. INTRODUCTION

Using IoT, sensor networks are developed which provides wide range of applications. A WSN consists of different number of nodes connected to a receiver which performs different tasks, which provides data delivery reliable for IoT based applications.

For data reliability, a new approach was developed using GOR which do not define the path for the routing before the transmission of data. The channel of the network has the nature of sharing and broadcasting the data over a multiple nodes of sensors. Hence in geographic opportunistic routing, the packets are forwarded using multiple candidates to which the sender will be defined the order with the priorities. This doesn't interrupt the transmission until the forwarder candidate transmits it successfully. Hence the performance of the GOR is better than the MR (multi-path routing), which doesn't interfere the signals present between the forwarder candidates.

The choice of the geographic routing is best over the traditional routing, as this doesn't needs to maintain the established paths between the sinks and the source. Hence the combination of opportunistic routing and the geographic routing is named as geographic opportunistic routing. All the present methods of GORs provide high reliability but due to the attack of DoS they suffer. The opportunistic routing intensifies the DoS attacks that void the packets delivered to the receiver through multiple forwarder candidates by not getting lost due to the invalid signals that the attackers feeds with the intention of wasting the resources of network and to interrupt the networks normal operation. The same is validated and analysed both by theoretically and by the experimental result.

At first, a new mechanism for authentication which is lightweight is mandatory for the WSNs which reduce the sensors cost of computation and also reduce the delay of packet delivery. Next is the design of the priority restoration of the forwarder candidates for the data reliability and integrity. Then, to reduce incurred overhead, designing of scheme for the sharing of information verification between the forwarder candidates.

In this work, to protect against the DoS attack in networks, a selective authentication based geographic opportunistic routing (SelGOR) is proposed for IoT, whose purpose is signal packets reliability and authenticity. SelGOR analyses the wireless nodes by statistic state information to increase the data delivery efficiency. To safeguard the data integrity SelGOR controls algorithm which is based on an entropy-based selective authentication.

The next section converses the network model and security model. After this the protocol SelGOR is presented.

2. NETWORK AND SECURITY MODEL

A Multi-hop Wireless Sensor Network is considered here which consists of sensor nodes and receivers are installed for an application of IoT. Sensors nodes transmit and receive data when they are within the wireless transmission range [R]. The Euclidian distance [d] should be greater than the transmission range [R] to ensure the multi-hop communication. The sensor network is assumed as an intense network in which every sensor node has many number of neighbour nodes. But the energy issue is highly considerable in the WSN, hence the sinks are assumed like capable of handling powerful devices and the remaining sensor nodes are made to operate on limited batteries. Nodes receive the energy information of the neighbouring nodes based on beacon messages.

In this paper, much importance is given to the Network layer's data delivery performance. The modified MAC protocol is used to gain the coordination of candidate forwarders and this is recommended for the opportunistic routing which is based on ACK/RTS/CTS mechanism in the IEEE 802.11b.

The Public Key Infrastructure (PKI) is necessary for key management in the WSN for the purpose of Security protection.

Every sensor nodes are assumed to have a pair of ECDSA keys:

Key 1: For verification Public key

Key 2: Private Key for signing data packets.

Public keys are approved as legal identities of sensor node by a trusted Certified Authority (CA). The sink nodes' or application developers' acts as CA in the real deployment. The sensor nodes are assumed like they know the public keys of every node and at no time disclose private key to any other.

3. THE SECURITY MODEL

Here, it is given the designing of the most proficient delivery protocol which can provide the reliable data in WSNs. Hence, it is important to have all these properties for data packets.

Data Reliability:

The sensor node must confirm the data relayed authenticity the neighbouring nodes before the sending the data packet. If the authenticity is not ensured, sinks will receive many invalid data from DoS attackers and this leads to create disturbances in the normal operations of applications. WSNs need an authentication scheme to have the property of data integrity.

Non-repudiation:

This property involves authentication and it allows the sink to ensure the third party of data packets responsible by the sender node. The sinks are able to determine who has sent the data packet which is invalid and report attackers to trusted CAs.

Data Consistency:

The Data packets are subjected to lose for link failures because the wireless medium is of broadcast and shared nature. WSNs are not supposed to halt the IoT application operations even the effect of data loss is unavoidable. Hence, it is necessary to have reliable data delivery protocol.

DoS attacks Resistant

DoS attackers send many invalid data packets, if there is no authentication scheme. This leads to lose network communication resources and upsets the normal data delivery. Normally, the computational resource and energy resource is less in number in sensor nodes. The scheme of authentication should have lesser cost of computational for WSNs energy efficiency to secure against DoS attackers.

4. METHODOLOGY

The outline of the selective authentication based geographic opportunistic routing is given in the Figure 1.

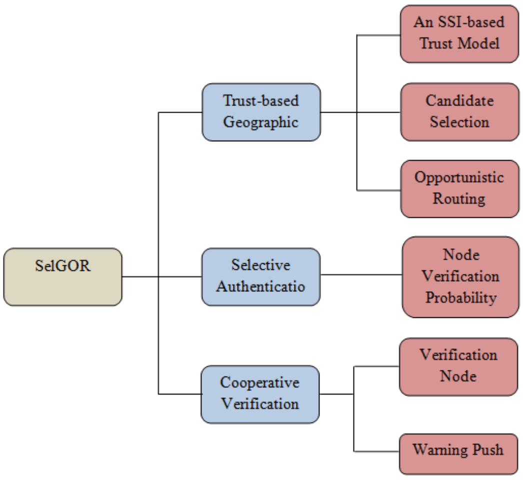

FIGURE 1. The SelGOR outline.

The SelGOR [figure 1] mainly consists of three components:

1. Trust-based geographic opportunistic routing,
2. selective authentication algorithm and
3. Cooperative verification scheme.

The three components are described as follows.

Trust-based Geographic opportunistic routing: The Sensor nodes create a trust model which is based on SSI and updates it in WSNs. This can be done by analysing the historical transmission data of wireless links. When the data packet reaches a sensor node, the sensor nodes have to identify the candidate forwarder which has set from the neighbouring nodes. This is to deliver the reliable data in opportunistic routing. To ensure this, the sensor node fixes the priority to every forwarder candidate based on routing of metric and this is given on the trust model based on SSI. Hence, the trust based geographic opportunistic routing is made to have a trust model which is based on SSI, opportunistic routing and candidate selection.

Selective authentication algorithm:
The sensor node must ensure the authenticity to defend against DoS attacks of any data packet before sending it. An algorithm on Entropy of selective authentication is presented here which can block the unnecessary and data packets which are invalid without verifying all signatures on each hop. The sensor nodes checked the probability if it knows the information about a received signature.
Also, the node verification method is specified which can be adjusted

Cooperative verification scheme: The sensor node undermines the candidate forwarders priorities when it starts verifying a data packet before the transmission.
Therefore, the mechanism design of verification to notice to solve the issue is given. Once it is verified, we can make use of the warning push mechanism which shares the result which is verified between candidate forwarders for fast isolation.

ADVANTAGES

- Available at low cost
- Easy Installation
- Easy to maintain
- Increases the network lifetime

APPLICATIONS

The applications of this method can be seen in the fields like Smart Home, Medical and Military.

3. CONCLUSIONS

In this paper, the design of SelGOR scheme is given which assures the authentication of IoT and its reliability on application based on data delivery. SelGOR uses the statistic state information based trust model to the efficiency of data deliver in WSNs. To isolate DoS attackers an algorithm with Selective authentication is developed whose computational cost is low.

REFERENCES

[1] M. Salehi and A. Boukerche, "A novel packet salvaging model to improve the security of opportunistic routing protocols," Computer Networks, vol. 122, pp.163-178, 2017.
[2] C. Lyu, D. Gu, X. Zhang, S. Sun, Y. Zhang, and A. Pande, "SGOR: Secure and scalable geographic opportunistic routing with received signal strength in WSNs," Computer Communications, vol. 59, pp. 37-51, Mar. 2015.
[3] J. So, and H. Byun, "Load-balanced opportunistic routing for duty-cycled wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 16, no. 7, pp. 1940-1955, Jul. 2017.
[4] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Common. ACM, vol. 47, no. 6 pp.53-57, Jun. 2004.
[5] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: A survey," IEEE Wireless Communications, vol. 11, no. 6, pp. 6-28, Dec. 2004.
[6] L. Atzori, A. Iera, and G. Morabito, ''The Internet of Things: A survey,'' Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
[7] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, ''Internet of Things (IoT): A vision, architectural elements, and future directions,'' Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.
[8] 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.
[9] R. H. Weber, ''Internet of Things—New security and privacy challenges,'' Comput. Law Secur. Rev., vol. 26, no. 1, pp. 23–30, Jan. 2010.
[10] J. N. Al-Karaki and A. E. Kamal, ''Routing techniques in wireless sensor networks: A survey,'' IEEE Wireless Commun., vol. 11, no. 6, pp. 6–28, Dec. 2004.
[11] E. Felemban, C.-G. Lee, and E. Ekici, ''MMSPEED: Multipath multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks,''

IEEE Trans. Mobile Comput., vol. 5, no. 6, pp. 738–754, Jun. 2006.

[12] S. Li, R. K. Neelisetti, C. Liu, and A. Lim, ‘‘Efficient multi-path protocol for wireless sensor networks,’’ Int. J. Wireless Mobile Netw., vol. 2, no. 1, pp. 110–130, 2010.

[13] X. Huang and Y. Fang, ‘‘Multi constrained QoS multipath routing in wireless sensor networks,’’ Wireless Netw., vol. 14, no. 4, pp. 465–478, 2008.

[14] 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.

[15] R. Sanchez-Iborra and M. Cano, ‘‘JOKER: A novel opportunistic routing protocol,’’ IEEE J. Sel. Areas Commun., vol. 34, no. 5, pp. 1690–1703, May 2016.

[16] 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.