RESEARCH ARTICLE OPEN ACCESS

DISCRIMINATIVE ATHENDICATION BASED OPPERTUNISTIC ROUTING IN WIRELESS SENSOR NETWORK WITH TRUSTWORTHY PATH MECHANISM

K.E.Eswari MCA., M.Phil., M.E,, K.Indhu
(Associate professor, Department of MCA, Nandha Engineering College(Autonomous), Erode, Tamilnadu, India
Email: eswarisaravanan2001@gmail.com)
** (Final MCA, Department of MCA, Nandha Engineering College(Autonomous), Erode, Tamilnadu, India
Email: indhu.18cal08.nandhaengg.org)

****

Abstract:

Wireless Sensor Networks (WSNs) are widely used because the communication system within the Internet of Things (IoT). In addition to the services provided by WSNs, many IoT-based applications require reliable data delivery over unstable wireless links. To guarantee reliable data delivery, existing works exploit geographic opportunistic routing with multiple candidate forwarders in WSNs. However, these approaches suffer from serious Denial of Service (DoS) attacks, where a large number of invalid data are deliberately delivered to receivers to disrupt the traditional operations of WSNs. In this paper, we propose a selective authentication-based geographic opportunistic routing (SelGOR) to defend against the DoS attacks, meeting the requirements of authenticity and reliability in WSNs. By analyzing statistic state information (SSI) of wireless links, SelGOR leverages an SSI-based trust model to improve the efficiency of data delivery. Unlike previous opportunistic routing protocols, SelGOR ensures data integrity by developing an entropy-based selective authentication algorithm, and is in a position to isolate DoS attackers and reduce the computational cost. Specically, we design a distributed cooperative verication scheme to accelerate the isolation of attackers. This scheme also makes SelGOR avoid duplicate data transmission and redundant signature verication resulting from opportunistic routing. The extensive simulations show that SelGOR provides reliable and authentic data delivery, while it only consumes 50% of the computational cost compared to other related solutions.

Keywords —**Internet of Things, opportunistic routing, DoS attacks, selective authentication**

****

I. INTRODUCTION

Wireless sensor networks (WSNs) have been developed in the Internet of Things (IoT) and play an important role to provide a wide range of applications through sensors, such as smart home, trafic management, smart grids and environment monitoring [1], [2]. A wireless sensor network contains some receivers/sinks and a number of distributed sensor nodes which collaboratively collect and transmit data to perform a variety of missions. Built upon WSNs, providing reliable data delivery is usually expected for IoT-based applications. One example of such applications is smart healthcare, which is employed for the aim of monitoring, tracking or treating patients [3]. In this

application, sensor nodes collect he patient's physical data and then deliver them to the doctor. Based on the collected data, the doctor is aware of the physiological status of the patient, and is in a position to make a suitable diagnosis. The above application requires WSNs to provide reliable data delivery, which is regarded as the critical factor for the success of diagnosis. However, based on the varying and shared wireless mediums, WSNs are susceptible to link failures due to signal interference or signal fading, which may signicantly decrease the quality of service [4], [5]. Therefore, supporting reliable data delivery becomes a challenging problem in WSNs. To address this issue, many multi-path routing strategies [6] [8] have been proposed to improve the reliability of data delivery in WSNs. However, maintaining a multi-path route for a data ow has a high communication cost for the instability of wireless channels. Moreover, since data packets are transmitted over multiple paths to receivers, more transmission contentions and signal interferences are introduced leading to additional transmission failures in the network. Recently, an efficient approach to meet the requirement of data reliability is exploiting (geographic) opportunistic routing which doesn't determine the routing path before data transmission [9] [12]. With the broadcast and shared nature of the wireless channel, it allows packet transmission to be overheard by multiple sensor nodes. Instead of one singer for warder in traditional routing, multiple candidate forwarders are selected within the opportunistic routing, which are ordered based on the priorities denied by the sender of the packet. Therefore, the packet transmission is not disrupted as long as one candidate in the forwarder set successfully relays it.

II. RELATED WORK

There have been many researches on opportunistic routing exploiting the spatial diversity of wireless transmissions for data delivery in wireless unplanned networks.As one branch of opportunistic routing, geographic opportunistic routing which makes use of the geographic location to choose the candidate forwarders in the neighbour list is also widely studied in the literature Sanchez-Iborra and Cano propose the opportunistic routing named JOKER so as to balance the tradeoff between multi-media service and energy consumption for mobile devices. Their JOKER uses the routing metric combining the reliability of wireless links with the distances to receivers for candidate selection. To minimize the energy consumption and maximize the lifetime of WSNs, Luo et aloptimize the candidate forwarder set based on the distances to receivers and therefore the remaining energies of sensor nodes, then use opportunistic routing for data delivery in the model of one-dimensional queue network. So and Byun design an opportunistic routing for load balance in the duty-cycled wireless sensor networks. In their scheme, the number of candidate forwarders is controlled supported the estimation of forwarder cost so as to scale back redundant data forwarding caused by the opportunistic routing. Zeng et al. propose a geographic opportunistic routing in the multi-rate wireless networks. They study the strategies of candidate selection and candidate coordination, and then design an effective metric for the opportunistic routing to achieve high network throughput. Cheng et al. address the problem of Quality of Service (QoS) provisioning with the constraints of reliability and end-to-end delay in WSNs. They formulate it as an optimization problem, and then design an efcient geographic opportunistic routing to provide QoS with low communication cost. Although these works are on the idea of opportunistic routing, they mostly address the issues of QoS, load balance or energy efciency. In terms of security, Salehi and Boukerche address black hole attacks on opportunistic routing in the wireless mesh networks, where nodes deliberately drop the info packet that they're alleged to transmit.

III. NETWORK AND SECURITY MODEL

A. NETWORK MODEL

We assume a multi-hop WSN which consists of variety of sensor nodes and a few sinks/receivers is deployed for one application of IoT. Sensor nodes within the wireless transmission range R could directly send data to each other. The multi-hop communication is enabled when their Euclidian distance is greater than the transmission range. We assume that the sensor network is a

dense network, where each sensor node has plenty of neighbor nodes. Thus, this network can be denied by a graph G (V; L), where V depicts the set of sensor nodes and L depicts the set of direct links between sensor nodes. We denote a link li;j 2 L if the Euclidian distance between the sender nodes i 2 V and the receiver node j 2 V is less than the wireless transmission range R. We assume sensor nodes are stationary, and know their location information and the position information of sinks. Besides, nodes are aware of the location information of their neighbor nodes through beacon messages within the general geographic routing, i.e., a sensor node periodically broadcasts its identity, location information and residual energy in beacon messages [13]. As the energy issue is a major challenge in the WSN, we assume that sinks are equipped with powerful devices and other sensor nodes operate on limited batteries. Based on beacon messages, it is feasible for nodes to obtain the energy information of their neighbor nodes. In this work, we mainly concentrate on the performance of data delivery in the network layer. To achieve the coordination of candidate forwarders in our protocol, we exploit a modied MAC protocol which is proposed for opportunistic routing based on RTS/CTS/ACK mechanism in the IEEE 802.11b [15]. However, other MAC layer problems such as hidden terminal or collision avoidance aren't considered in this paper. For security protection, a Public Key Infrastructure (PKI) is required for key management in the WSN [36].We assume each sensor node features a pair of ECDSA keys: a public key for verication and a personal key for signing data packets. A trusted Certicate Authority (CA) would endorse the public keys as legal identities of sensor nodes. In the real deployment, sink nodes or developers of applications could act as the role of CA. We assume each sensor node knows the public keys of all nodes, and never releases its private key to another party.

B. SECURITY MODEL

In this paper, our goal is to design an efficient and reliable data delivery protocol which technically maintains the desired authentic data in WSNs. Therefore, we should provide these important properties for data packets.

1) DATA INTEGRITY

Before transmitting a data packet, a sensor node is supposed to ensure the authenticity of data relayed by its neighbor nodes. Otherwise, sinks would receive many invalid data from the DoS attackers, which disrupts the normal operations of applications. To provide the property of data integrity, an authentication scheme is indispensable for WSNs.

2) NON-REPUDIATION

The property of non-repudiation usually involves authentication. It permits a sink to convince third parties that the sender node is responsible for the data packet. According to this property, sinks can ascertain the sender of any invalid data packet and report attackers to trusted CAs.

3) DATA RELIABILITY

Because of the printed and shared nature of the wireless medium, data packets are susceptible to lose for link failures. Even the effect of data loss is inevitable in WSNs, it should not disable the operations of applications based on IoT. Therefore, it's essential to ensure high reliability for any data delivery protocol.

4) DOS ATTACKS RESISTANT

Without any authentication scheme, the DoS attackers may send tons of invalid data packets within the network to waste communication resources of networks or disrupt the normal data delivery. Moreover, sensor nodes normally have limited computational and energy resources. To defend against DoS attackers, the authentication scheme should have low computational cost for energy efficiency in WSNs. We consider each sensor node registers with the CA by preloading a public/private key pairs: PK and SK. The private key SKi is exploited by the sender node i to sign the data packet.

IV. SELECTIVE AUTHENTICATION BASED GEOGRAPHIC OPPORTUNISTIC ROUTING.

In this section, we _rst give an overview of our selective authentication based geographic opportunistic routing, and then describe its primary components.

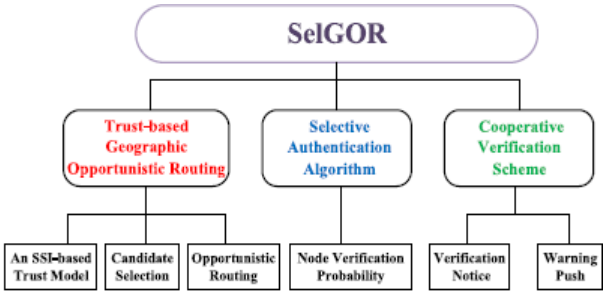

FIGURE 1. The overview of SelGOR.

PROTOCOLOVERVIEW

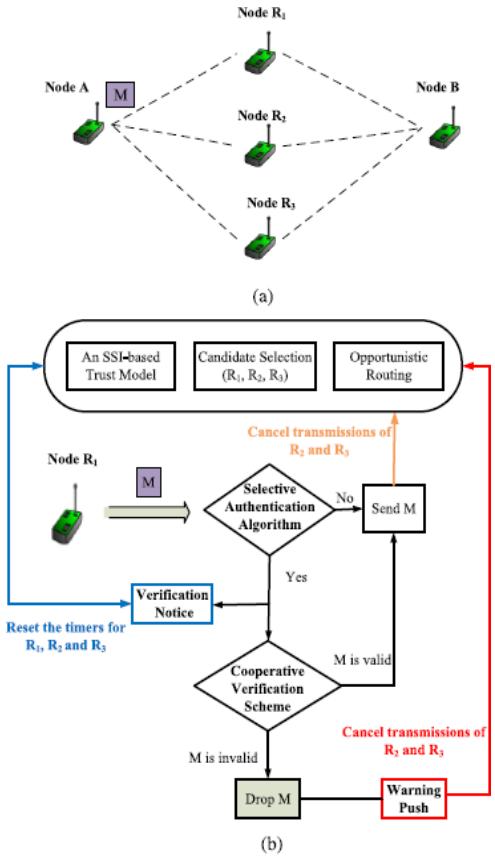

FIGURE 2. The illustration of SelGOR. (a) The network topology.(b) The work flow of node R1.

When M arrives at node A, the relay node A would deter-mine the priorities of candidate nodes supported the routing metric, which is made supported the SSI-based trust model. In our example, we assume that the decided order is fR1; R2; R3g, which indicates nodes would forward M with the priority rule (R1 > R2 > R3). The priority rule is usually realized by the distinctive timer run on each candi-date node [10], [15]. Accordingly, node R1 becomes the first candidate node to relay the info packet. If the link quality ispoor, it cannot receive M and therefore the transmission is interrupted. However, because of the shared wireless channel, node A and other candidate nodes don't hear any packet transmission from node R1 at this moment, and so detect the failure of the wireless link. Node A adjusts the trust of link lA;R1 within the SSI-based trust model. Meanwhile, node R2 is activated to transmit M. When its timer expires, node R2 becomes the relay node of M with the principle of opportunistic routing. Providing that node R1 receives the packet M correctly, it performs selective authentication algorithm to come to a decision to 31072 VOLUME 7, 2019 ***C.*** Lyu et al.: SelGOR in WSNs for IoT Against DoS Attacks check M or not. If it skips the verification process supported the node verification probability of node A, the info packet is promptly transmitted to the following relay node. supported the scheme of opportunistic routing, node R2 and R3 cancel the transmissions of M by disabling their own timers. However,if it decides to verify M, a packet of verification notice should be multicast to the opposite candidates with low priorities in order to reset their timers. After finishing verifcation,node R1 sends out M to the following relay node if it's valid. Concurrently, node R2 and R3 disable their timers to cancel the transmissions of M. just in case M doesn't pass the verification, node R1 drops M and increases the node verification probability of node A.

B.TRUST-BASED GEOGRAPHIC OPPORTUNISTIC ROUTING

Our trust-based geographic opportunistic routing consists of an SSI-based trust model, candidate selection and opportunis-tic routing to supply reliable data delivery. First, we design an SSI-based trust model by characterizing unreliable wire-less links in WSNs. Second, we integrate the SSI-based trust model into our routing metric to pick multiple candidates from neighbor nodes. At last, we describe the scheme of opportunistic routing.

1) SSI-based trust model

By collecting and analyzing historical data transmission of neighbors, we exploit the ratio of the amount of packets successfully delivered to the quantity of packets sent to char-acterize the trust of a link. At a high level, a sensor node k divides the timeline into a series of observation intervals, which has the identical length of n. During each observation interval, it's possible for node k to listen to the wireless channel and check whether an information packet is really forwarded by the selected neighbor node.

$$T_k^i(n) = \frac{NS_k^i(n)}{ND_k^i(n)}. \qquad (1)$$

$$T_k^i(t) = \omega T_k^i(t-n) + (1-\omega)T_k^i(n), \qquad (2)$$

2) Candidate Selection

In opportunistic routing, many routing metrics are developed within the literature to pick out candidates for load balance,energy saving or QoS provisioning in WSNs. By jointly considering the proposed techniques and unreliable wireless links, we mainly exploit three factors to style our routing metric, including the single-hop distance progress the trust degree and therefore the remaining energy of the neighbour node.

$$SP_k^i = D(k,s) - D(i,s), \qquad (3)$$

$$RM_k^i = \gamma(SP_k^i \times T_k^i) + (1-\gamma)RE^i, \qquad (4)$$

3) Opportunistic Routing

After candidate selection, the source/intermediate node k is ready to send an information packet to the sink. It first performs the selective authentication algorithm to make a decision to check the information packet or not. When it skips the verification process or the verification result's true, it broadcasts the data packet, which has the list of candidates and their priorities in line with Ck. within the opportunistic routing, each candidate forwarder follows the assigned priority to forward the data packet, as shown in Algorithm 1. After receiving the info packet correctly, a candidate node i starts a timer time(i) = Order(i), where could be a constant and Order(i) is its priority defined within the data packet.

C.SELECTIVE AUTHENTICATION ALGORITHM

Before sending a knowledge packet, each sender node signs the information packet with its ECDSA private key so as to produce the security properties of knowledge integrity and non-repudiation in WSNs. To preserve the computational and energy resources, relay nodes often forward data packets without verification until the sink node checks the signatures of information packets. However, such a forwarding scheme is susceptible to DoS attacks, where attackers send an oversized number of bogus datapackets with illegal signatures to waste the network resources and disrupt the traditional operations of WSNs. Especially, opportunistic routing makes DoS attacks more serious that invalid data packets are reliably delivered with multiple candidate forwarders. The scheme of checking signatures on every node can block the invalid data packets, but it immensely extends the delivery delay and is computationally expensive.

Algorithm 1 Procedure of Opportunistic Routing Run by Candidate Nodes.

Input: a data packet broadcast to N candidate nodes with their priorities defined by the sender k
Output: successful and coordinated data delivery

1: **if** Node $i \in C_k$ **then**
2: Receive the data packet;
3: Start a timer and $time(i) = \tau * Order(i)$, where τ is a constant and $Order(i)$ is the priority of node i defined in the data packet; // $Order(i) = 0, 1, \cdots, N-1$
4: **end if**
// Node i is selected as the first candidate node;
5: **if** $time(i) == 0$ **then**
6: Node i becomes the next-hop sender, which is ready for data transmission;
7: **return**
8: **end if**
// Node i is not selected as the first candidate node;
9: **while** $time(i)! = 0$ **do**
10: **if** Node i overhears that the data packet is being transmitted by another candidate node; **then**
11: Cancel the timer $time(i)$ and drop the data packet;
12: **return**
13: **end if**
14: **end while**
// The timer of node i expires
15: Node i becomes the next-hop sender, which is ready for data transmission;
16: **return**

verified with a lower probability when the sensor node knows more information about the forwarder. Hence, forwarder or neighbor identification should be supported in our algorithm.There are many efficient schemes for neighbor identification (e.g., TESLA [35]), our algorithm works with all of them.As the measurement of uncertainty, node verification probability is exploited to achieve isolation of attackers, which could be adjusted dynamically according to received invalid signatures.

Algorithm 2 Procedure of Cooperative Verification Run by Candidate Nodes.

1: **if** Node $i \in C_k$ becomes the next-hop sender **then**
2: Perform selective authentication algorithm with the output of a flag;
3: **if** The flag indicates verification **then**
4: Broadcast a packet of Verification Notice;
5: Verify the data packet;
6: **if** The data packet is invalid **then**
7: Increase node verification probability;
8: Broadcast a packet of Warning Push;
9: Drop the data packet;
10: **else**
Send the data packet with opportunistic routing;
11: **end if**
12: **else**
Send the data packet with opportunistic routing;
13: **end if**
14: **else**
15: **if** Node i receives Verification Notice **then**
16: Increase its timer;
17: **end if**
18: **if** Node i receives Warning Push **then**
19: Increase node verification probability;
20: Stops its timer and drop the data packet;
21: **end if**
22: **end if**

D.COOPERATIVE VERIFICATION SCHEME

Our cooperative verification scheme is proposed to optimally integrate the selective authentication algorithm into trustbased geographic opportunistic routing. When a sensor node decides to verify a knowledge packet, it breaks down the priorities of candidate forwarders defined by the opportunistic routing. This is because the verification time of a signature is way greater than the TRM [18]. Therefore, we design the mechanism of verification notice to revive the priorities of candidate forwarders in opportunistic routing. which mainly consists of the mechanism of verification notice and therefore the mechanism of warning push.

1) Verification NoticeBased on node verification probability, if a sender or a relay node decides to verify a knowledge packet before transmission, it will broadcast a packet of verification notice, which incorporates its identity, the information packet's identifier (i.e., the identity of source node and therefore the sequence number), the identities of

candidate nodes withlow priorities and also the estimation of the verification time.

2) Warning Push If a knowledge packet's signature agrees with the general public key of the source node, it'd be considered to be a sound data packet,and then forwarded by the relay node with opportunistic routing. Otherwise, it fails the verification and is dropped by the relay node. If an invalid signature is detected, the relay node adjusts the node verification probability of its preceding forwarder. As illustrated in Figure 2, the relay node R1 increases the node verification probability of node A if M is invalid. Besides, a packet of warning push which contains the relay node's identity, the information packet's identifier, the identity of the preceding forwarder node and also the identities of candidate nodes with low priorities, is broadcast by the relay node.

V. PRELIMINARY ANALYSIS OF AUTHENTICATION

Since each sender signs every data packet with its private key, the signature of the info packet ensures the properties of data integrity and non-repudiation. rather than checking every signature on the sensor node, we exploit the selective authentication algorithm to cut back the computational cost in SelGOR. Here, we study the effect of selective authentication algorithm, and consider an easy line model for simple modeling. As shown in Figure 3, we assume sensor nodes are placed at location 0, d, 2d, Ld. The transmission range R is ready to Nd. Therefore, each node has N candidate nodes for data forwarding. The DoS attacker is found at the origin location, and sends an invalid signature at intervals. We consider the attacker sends a sound signature to avoid being detected at the beginning (i.e., g = 0), then sends invalid signatures after the first measure (i.e., g = 1).When a candidate node i2 Cs receives a knowledge packet from the sender s, it verifies the signature with the verification probability of vs i .

$$F_{OR}(g,h) = g * \prod_{s=0}^{h-1}(1 - \prod_{i=0}^{N-1} v_i^s), \quad (5)$$

$$F_{SelGOR}(g,h) = g * \prod_{s=0}^{h-1}(1 - v_0^s), \quad (6)$$

where vs 0 indicates the node verification probability of the first candidate node. Considering that the initial node verification probability is set to v0 for all nodes, we compare the impact of authentication on our SelGOR thereupon on primary opportunistic routing in Figure 4. The analysis result shows that SelGOR can converge sooner than the first opportunistic routing with the selective authentication algorithm. As h increases, the quantity of invalid signatures in Equation (6) decreases much faster than that in Equation (5), since the mechanism of warning push accelerates the isolation process.

VI. PERFORMANCE EVALUATION

In this section, we perform simulation experiments to judge the performance of SelGOR under the DoS attacks in OPNET network simulator. We first describe the simulation setup. Second, we show the reliability of SelGOR, and compare it with other three routing protocols under different link qualities. Third, we study the performance of SelGOR with different parameters. Finally, we offer the simulation results to demonstrate the effectiveness of authentication achieved by SelGOR.

VII. CONCLUSION

In this paper, we designed an efficient scheme SelGOR aiming to provide the properties of authenticity and reliability of data delivery for IoT-based applications. As a trust-based geographic opportunistic routing, SelGOR exploits the SSIbased trust model to boost the reliability of information delivery in WSNs. To defend against DoS attacks, we studied the existing authentication schemes and located that they failed to operate for opportunistic routing thanks to either being unserviceable or high computational cost in WSNs.

REFERENCES

[1] L Atzori, A Iera, and G Morabito, “The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787-2805, Oct. 2010.
[2] J. Gubbi, R. Buyya, S. Marusic, and M.Palaniswami, “Internet of Things
(IoT): A vision, architectural elements, and future directions," Future generation computer systems, vol. 29, no. 7, pp. 1645-1660, 2013.
[3] L. D. Xu, W. He, and S. Li, “Internet of Things in industries: A survey,"
IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233- 2243, Nov. 2014.
[4] R. H. Weber, “Internet of Things-New security and privacy challenges," Computer Law & Security Review, vol. 26, no. 1, pp. 23-30, Jan. 2010.
[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] 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 Transactions on Mobile Computing, vol. 5, no. 6, pp. 738-754, Jun. 2006.
[7] S. Li, R. K. Neelisetti, C. Liu, and A. Lim, “
Efficient multi-path protocol for wireless sensor networks," International Journal of Wireless and Mobile Networks, vol. 2, no. 1, pp. 110-130, 2010.
[8] X. Huang and Y. Fang, “Multiconstrained qos multipath routing in wireless sensor networks," Wireless Networks, vol. 14, no. 4, pp. 465-478, 2008.
[9] G. Schaefer , F. Ingelrest, M. Vetterli, “Potentials of opportunistic routing in energy-constrained wireless sensor networks," in Proceedings of the 6th European Conference onWireless Sensor Networks, February 11-13, 2009, Cork, Ireland.
[10] R. Sanchez-Iborra and M. Cano, “JOKER: A novel opportunistic routing protocol," ," IEEE Journal on Selected Areas in Communications, vol. 34, no. 5, pp.1690-1703, May 2016.
[11] 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.