Identity-based Scheme Against Sybil Attacks in Wireless Sensor Networks

V. Sujatha, E.A. Mary Anita

Abstract— Wireless sensor networks are insecure against various security attacks. One such harmful, yet easy to promote an attack is the sybil attack which creates multiple identities to achieve access to the wireless sensor networks. A new identity based scheme to provide security against Sybil attacks is proposed in this paper. It detects as well as broadcast information about the attackers to all the nearby sensor nodes. Expensive MapToPoint and pairing operations are not used in this scheme to reduce overheads. It also provides other essential security features. Aggregate-verification to verify several messages at the same time is also proposed in this paper. The performance of the proposed scheme is compared with other recent schemes and the results show that the proposed scheme has reduced amount of overheads and better performance.

Keywords—AODV, Black Hole Attack, Hash Function, Security, VANET.

I. INTRODUCTION

Due to the extensive variety and range of applications in health care and military surveillance applications, the wireless sensor network attracts a lot of consideration and attention. Many wireless sensor networks are deployed in deserted areas which are not supervised. Hence, such networks should be deployed in a secure way with essential security requirements. On the other hand, the main constraints like storage issues, power consumption, etc. should also be considered while establishing sensor networks.

They are exposed to various outbreaks like several attacks. One among the destructive attack is Sybil attack, in which attackers create numerous identities to get in to the network. Such multiple identities which are generated to act as multiple nodes are known as Sybil nodes. It is most harmful, yet easily launched attacks in wireless sensor networks. It also acts as a gateway for other attacks like wormhole attacks, sinkhole attacks, etc.

Sybil attack [20] operations are done by using different methods like direct & indirect communication, stolen & fabricated identities and simultaneous & non-simultaneous attacks. In direct communication, Sybil nodes communicate directly with the honest nodes, while intermediate nodes are used in the indirect methodto establish communication with legitimate nodes in the network. In stolen & fabricated identities method, Sybil nodes either use stolen identities to impersonate as a legitimate node or it fabricates the stolen identities to create new identities. In simultaneous and non-simultaneous attacks, multiple identities are created by Sybil nodes and used either simultaneously at the same time or used one by one at different times. In this way Sybil operations are carried out at the wireless sensor networks.

Sybil attacks of different types are launched in wireless sensor networks [1] by using the aforementioned methods : Distributed storage, routing, data aggregation, voting and misbehavior detection. In distributed storage, attacks occur in data fragmentation and replication where IDs will be fragmented/replicated and stored in the sink node. If Sybil nodes gain access to the network, such IDs will also be stored in Sybil nodes by considering it as legitimate sink nodes. In routing method, messages are broadcast in multiple paths with Sybil nodes. In data aggregation, the data got from sensor nodes are gathered and transmitted to the sink nodes. Sybil nodes can also acquire access to such aggregated data in the network. Voting involves identifying attackers in the networks. In such cases, Sybil nodes will vote legitimate nodes as attackers. It can also frame the legitimate nodes with its misbehaviors. In this way, Sybil attacks are launched in the wireless sensor networks.

With the increase in different types of Sybil attacks, researchers focus mainly on mitigating such attacks to establish secure communication in the network. Most of the methods use different cryptographic operations to identify sybil attackers in the network. The localizations methods are also used to identify Sybil nodes by using the position of the nodes in the network. RSSI (Received Signal Strength Indicator) is the main parameter used in most of the schemes to identify Sybil nodes in the network. In this paper the identity based scheme is used to recognize the attackers in Wireless sensor network.

The following is our contribution in this paper.

•A new identity based scheme is proposed to provide security against Sybil attacks in wireless sensor networks.

•Expensive MapToPoint and pairing operations are not used in this scheme to reduce overheads.

•It also provides other security features like message integrity, unlinkability and message authentication.

•It is also secure against other security attacks based on authentication and message integrity.

The remaining paper is arranged as follows: Sybil attack detection and prevention existing techniques are discussed in Section II. The proposed scheme is elucidated clearly in Section III and security analysis is discussed in Section IV. The performance with the simulation results of the proposed scheme is analyzed in Section V. In Section VI conclusion is presented.

Revised Manuscript Received on October 15, 2019

V. Sujatha, AMET University, Chennai, Tamilnadu, India.

E.A. Mary Anita, Professor, Department of IT , S.A. Engineering College, Chennai, Tamilnadu, India.

II. RELATED WORK

Different schemes are proposed to detect sybil attacks in wireless sensor networks. Most of the schemes are based on localization techniques and identity based schemes. Some of the Sybil attack detection techniques proposed by different authors are discussed in this section. Lazos et al. [2] proposed range-independent localization scheme for wireless sensor networks. Here, locators are used to identify sybil nodes in the network. Locators has high-power directional antennas whose locations are known and it is fully trusted. It sends beacon information with its location to all the nearby sensor nodes. Sensor nodes compute its approximate location by using the locators position. Neighbor locator density is used as a parameter to identify Sybil nodes in the network. The main problem is that it needs additional hardware requirements which is quite expensive. Improvisation of this scheme is done in [3] which use rotational antennas and multiple transmission power levels to detect Sybil nodes in the network, however it increases computation and communication overheads.

Demirbas et al. [4] proposed a RSSI centered scheme to identify the Sybil attackers in the network. Received signal strength (RSS) is measured for each message and stored. Three cooperating nodes exchange its stored values and compute its ratio. If the differences of ratio are within the predefined threshold value, then the sender is identified as Sybil node. It has storage issues which are its main drawback. Wen et al. [5] use Time Difference of Arrival (TDOA) method is used to distinguish sybil nodes from legitimate nodes in the network. Each node has its own TDOA ratio, which is associated with the identity of the sender node. If two identities of the senders have same TDOA ratio then it is identified as a Sybil node.

Zhang et al. [6] proposed Angle of Arrival (AOA) based trust scheme to recognize Sybil nodes in the network. It uses AOA as a parameter to recognize Sybil nodes in the network that multiple Sybil identities generated from a Sybil node will be in the same location. If the signal phase difference between the adjacent nodes is below the threshold value, then it is identified as Sybil node. Wang et al. [7] proposed a disseminated localization algorithm known as TMCA to detect Sybil as well as other attackers in the network. It is based on the concept of non-beacon neighbor nodes cooperations.

Yuan et al. [8] proposed a new localization based scheme against Sybil attack known as Sybil-Free Approximate Point in Triangulation centered localization scheme (SF-APIT). It improves the accuracy of the APIT localization scheme. The main benefit of this scheme is that it need not provide additional hardware support. It also has less communication overheads. By using this scheme, sensor nodes acquire accurate location information and thereby Sybil nodes are easily identified. Zhan et al. [9] introduced a trust based routing scheme for wireless sensor networks. It provides security against different attacks like Sybil, sinkhole and wormhole attacks. It is used in dynamic wireless sensor networks. It affords most trusted and energy-efficient route. Based on the trust levels of the neighbor nodes, routes are established to the sink nodes. The trust level of a node is portrayed as a decimal number within [0,1]. By using this trust values, attackers in the networks are easily identified.

Different identity based schemes [10] – [19] are also proposed for different networks which are used for various applications like health care monitoring systems, environmental monitoring systems, security systems, etc.,. But it has high computation and communication overheads because of the usage of expensive pairing operations for verification purpose. Hence, identity based schemes without pairing operations are proposed to reduce overheads [13], [14], [17]. Even though the computation and communication overheads are reduced when compared to that of schemes with pairing operations it still have high overheads. Hence a new identity based scheme with less overheads is proposed in this paper.

III. PROPOSED SCHEME

An identity based scheme is proposed to provide security against Sybil attacks in wireless sensor networks. Elliptic Curve Cryptography (ECC) is used to sign the messages to be transmitted to other nodes. Expensive MapToPoint and pairing operations are not used in this scheme to reduce overheads. Initially, each node will be assigned an ID with other parameters to sign and verify messages. Messages are signed using its private key and other attributes which will be verified by the receiver. Aggregate-verify is also proposed which helps to certify several messages at the same time after aggregation. The proposed scheme is explained in detail in the section. It has five phases, they are: setup, private key generation, message signing, verification and aggregate verification phase. The notations used in this scheme are given in Table 1.

Notation	Description
P	Generator Point
H, H1	One-way hash function
ki, ri	Random numbers
Si	Private key
ID	Identity of node
T	Timestamp
M	Message

Table 1: Notations Used

A. Setup Phase

Let F_n be the finite field with parameters a,b of the elliptic curve E ($y^2 = x^3 + ax + b \pmod n$, where $4a^3 + 27b^2 \neq 0$). Let P be the originator point of E and H: $\{0,1\}^* \rightarrow Z_q$, H_1: $\{0,1\}^* \rightarrow Z_q$ be two hash functions. These parameters will be loaded in all legitimate nodes, {P, H, H_1, ID} where ID is the identity of the node.

B.Private Key Generation

Each node will compute,

$K_i = k_i P(1)$

$S_i = H (ID) k_i(2)$

Where ki is the random number and Si is the private key.

C. Message Signing

Before sending the sensed data, sensor nodes will sign messages to be transmitted. Message signing is carried out as follows.

$R_i = r_i P$(3)

$V_i = H_1 (K_i, R_i, ID, M, t) r_i + S_i$(4)

Where ri is the random number, t is the current timestamp and M is the message to be transmitted. Each node will send {ID, M, t, Ki, Ri, Vi} to its neighbor nodes.

D. Verification

When a message is received by a node from its neighbor node, it first verifies the message before accepting it and then it forwards it to its nearby nodes. The verification process is carried out as follows.

Vi P = (H1 (Ki, Ri, ID, M, t)) Ri + H (ID) Ki (5)

If the above equation is true, then the node is considered as a legitimate node and the data received is forwarded to other nearby sensor nodes. If the above equation is false, then the received message is discarded and the identity of the attacker node is broadcast to all its nearby nodes. Thereby, attacker nodes are isolated from the network and sensed data are not transmitted in the path with the attackers.

E. Aggregate Verification

The sensed data will be transmitted to sink node through intermediate nodes. Hence the sink node will receive n number of messages from other nodes. In such cases, sink node can verify all the n number of messages at the same time by using the aggregate-verification as follows. Let Ai = H1 (Ki, Ri, ID, M, t) and Bi = H (IDi), then aggregate verification is carried out as follows.

$$\left(\sum_{i=1}^{n} V_i\right) P = \left(\sum_{i=1}^{n} A_i R_i\right) + \sum_{i=1}^{n} B_i K_i \quad (6)$$

If the above equation is true, then the data received is considered as valid, and it is accepted by the sink node.

IV. SECURITY ANALYSIS

A. Security Proof

It is proved in this sub-section that the signing method used in the proposed scheme is unforgeable.

Definition 1 Elliptic Curve Discrete Logarithm Problem: Let S = s P and s € Zq, it is infeasible to find the value of s from S where P is the point generator.

Theorem 1: Let X be the number of questions asked by the algorithm A to random oracle. It is suggested that if an algorithm A can crack the proposed scheme, then there is an algorithm B which can break ECDLP.

Proof: Consider there is an illegitimate node A which can break the proposed scheme, then the algorithm B can break the ECDLP by using the illegitimate A.

Setup: It selects the parameters {P,ID,H,H1} and send it to the adversary node A. Let LH1 is the hash list maintained by algorithm B.

H1 hash query: A sends H1 hash query to algorithm B with parameters { Ki, Ri, IDi, Mi }. B checks its hash list LH1 for the parameter { Ki, Ri, IDi, Mi }, if it is already present in the hash list with the tuple h1 { Ki, Ri, IDi, Mi, h1 } then B will return the value of h1 to the adversary A, else it will push the parameter in the list with the tuple h1 and return h1.

Sign query: If A makes a sign query with message Mi and other parameters { Ki, Ri, IDi } then B will return the value of h1.

Analysis: Using Forking Lemma, if A constructs two valid signatures Vi = h1 ri + Si and Vi* = h1* ri + Si , h1 ≠ h1*, then B can compute the value of Si as follows

$(h_1^* V_i - h_1 V_i^*) / (h_1^* - h_1)$

$= (h_1 h_1^* r_i + S_i h_1^* - h_1 h_1^* r_i - S_i h_1) / (h_1^* - h_1)$

$= (S_i (h_1^* - h_1)) / (h_1^* - h_1)$

$= S_i$ (7)

From equation 7 it is proved that B can also solve ECDLP. Hence, the signing method proposed is unforgeable.

B. Resistance Against Security Attacks

Sybil attack is launched by using the aforementioned methods in section I. For example, if a node X use identities of node Y and Z to send messages to node A and B at the same time, both nodes A and B will identify node X as an attacker and forwards the information of node X to all its nearby nodes as an attacker. It is done by using the following steps.

Step 1: Node X sends fake message M with the identities of node Y and Z to A & B as follows.

Node X → A : { IDy, M, t, KY, RY, VX }

Node X → B : { IDZ, M, t, KZ, RZ, VX }

Step 2: In both the cases, node A and B will identify node X as the attacker and broadcast the information of the attacker node X as { IDA, M, t, KA, RA, VA },{ IDB, M, t, KB, RB, VB } to all the nearby nodes, where the message M has the information about the attacker node X. In this way the proposed scheme provides security against Sybil attacks.

C. Authentication

By theorem 1, it is shown that the proposed scheme is unforgeable. Hence it provides secure authentication in the network.

D. Message Integrity

The signing method of the proposed scheme uses the message as one of the parameters to compute a hash function as shown in the equation 4. Hence, if the message is altered, it will be detected in the verification phase. Thus the proposed scheme ensures message integrity.

E. Unlinkability

The messages signed are unlinkable to one another. Since different parameters are used to sign a message, the signed value will be different and it cannot be linked.

V. PERFORMANCE EVALUATION & RESULTS

In this section, the performance of the proposed scheme is appraised by comparing it with other recent schemes.

A. Computation Overhead

The proposed scheme is compared with recent schemes [10], [12], [11], [15], [16], [13], [14], [17]. Among these schemes [10], [12], [11], [15], [16] use expensive pairing operations for verification and schemes [13], [14], [17] verifies without using expensive pairing and MapToPoint operations. The computation cost of different cryptographic operation is given in the table 2 [17].

The computation cost for message signing is given in the table 3. As shown, the proposed scheme has less computation overheads when compared to that of other schemes.As shown schemes [13] [14] [17] and the proposed scheme has the same computational cost for signing a message, whereas it is 91.4%, 91.4%, 96.59%, 95.37% and 96% less than that of other schemes [10], [12], [11], [15], [16]. It is graphically represented for 'n' number of messages in figure 1. As shown in the figure, the proposed scheme has reduced amount of computation overheads for message signing.

Operation	Symbol	Running Time (ms)
Bilinear Pairing Computation	T_{pr}	4.2110
Pairing-based Scalar Multiplication	T_{psm}	1.7090
Pairing-based Point Addition	T_{ppa}	0.0071
Scalar Multiplication on Elliptic Curve	T_{sm}	0.4420
Point Addition on Elliptic Curve	T_{pa}	0.0018
Map-to-point Hash Function	T_{mtp}	4.4060

Table 2: Running Time of Different Cryptographic Operations

Schemes	Sign
[10]	$3T_{psm}+2T_{ppa}$ (5.1412ms)
[12]	$3T_{psm}+2T_{ppa}$ (5.1412ms)
[11]	$5T_{psm}+3T_{ppa}+1T_{mtp}$ (12.9723ms)
[15]	$3T_{psm}+2T_{ppa}+1T_{mtp}$ (9.5472ms)
[16]	$4T_{psm}+2T_{ppa}+1T_{mtp}$ (11.2562ms)
[13]	$1T_{sm}$ (0.4420ms)
[14]	$1T_{sm}$ (0.4420ms)
[17]	$1T_{sm}$ (0.4420ms)
Proposed Scheme	$1T_{sm}$ (0.4420ms)

Table 3: Computation Cost for Message Signing

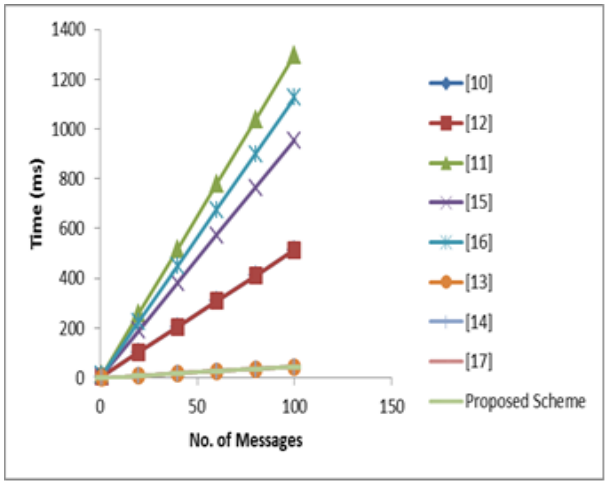

Figure 1: Computation cost of message signing

The computation cost of aggregate verification is given in table 4. The computation cost to verify a single message in the proposed scheme is 3Tsm + 1Tpa (0.4438ms) whereas the computation cost of aggregate verification is (2n+1)Tsm + 1Tpa. As shown, the proposed scheme has less computation overheads for aggregate verification when compared to that of other schemes. It is graphically given in figure 2. As shown, when the number of messages, n=100, then the proposed scheme has 88.85%, 85.81%, 88.92%, 85.91%, 88.91%, 0.6%, 0.79%, 33.57% less than other schemes [10], [12], [11], [15], [16], [13], [14], [17]. Hence the proposed scheme has less computation cost for message signing and verification.

B.Simulation Scenario

The proposed scheme is simulated in NS2 with 225 sensor nodes in the operating region of about 5000 x 5000m. Sybil attackers are manually placed and the performance of the system is evaluated in the existence and non-existence of attackers in terms of packet delivery ratio (PDR) and delay.

Schemes	Aggregate-Verify
[10]	$3T_{pr}+2nT_{psm}+(3n-2)T_{ppa}+nT_{mtp}$
[12]	$3T_{pr}+nT_{psm}+(3n-2)T_{ppa}+nT_{mtp}$
[11]	$3T_{pr}+2nT_{psm}+(4n-2)T_{ppa}+(n+1)T_{mtp}$
[15]	$3T_{pr}+nT_{psm}+(3n-2)T_{ppa}+(n+1)T_{mtp}$
[16]	$3T_{pr}+2nT_{psm}+(3n-2)T_{ppa}+(n+1)T_{mtp}$
[13]	$(2n+1)T_{sm}+(3n-1)T_{pa}$
[14]	$(2n+1)T_{sm}+(4n-1)T_{pa}$
[17]	$(3n+1)T_{sm}+(4n-1)T_{pa}$
Proposed Scheme	$(2n+1)T_{sm}+1T_{pa}$

Table 4: Computational Cost for Aggregate-Verification

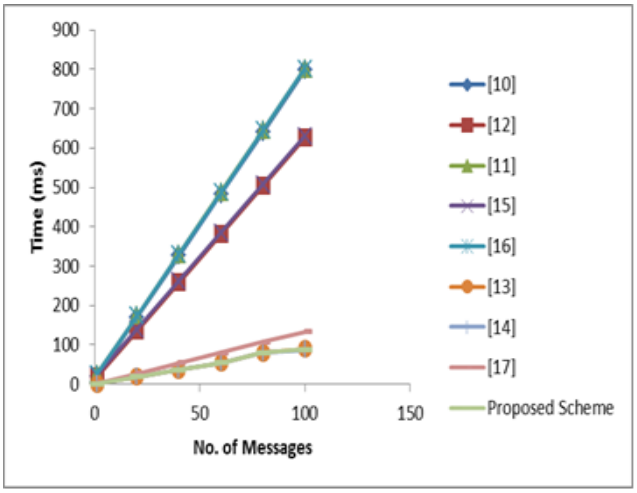

Figure 2: Computational cost of Aggregate-verification

Packet Delivery ratio (PDR) is the percentage of the difference between the number of packets sent and received to that of the number of packets sent. It is computed by using the formula given below.

PDR = ((No. of packets sent – No. of packets received) / No. of packets sent) * 100

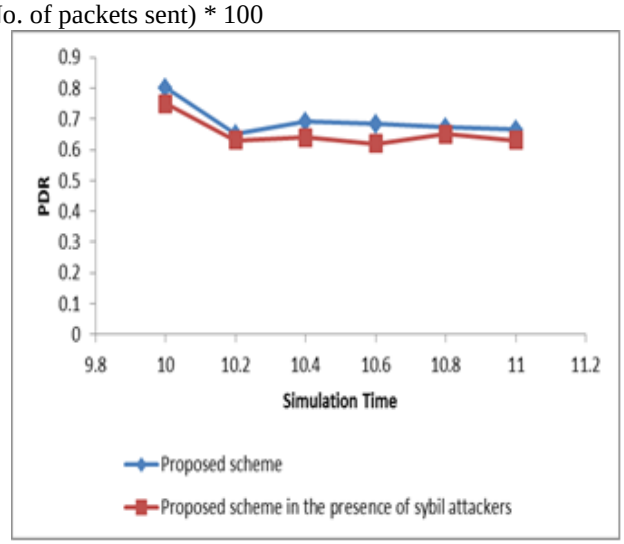

Figure 3: PDR vs Time

Figure 3 shows the PDR of the proposed scheme in the presence and absence of Sybil attackers. As shown in the figure, due to the presence of the Sybil attackers, PDR of the proposed scheme (on an average) is reduced by 11.3%. Since the proposed scheme identifies and rejects Sybil attackers efficiently, it is acceptable.

Delay is the time difference between the packet received time and the packet sent time. It is computed by using the formula given below.

Delay = Packet received time – packet sent time

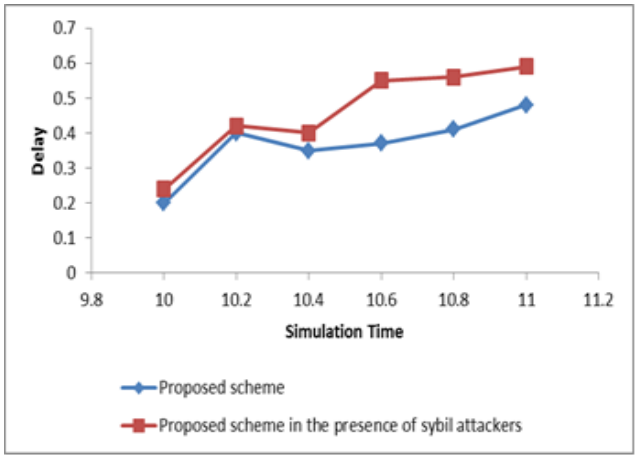

Figure 4: Delay vs Time

Figure 4 shows the delay of the proposed scheme in the presence and absence of Sybil attackers. As shown, because of Sybil nodes the time taken by the packets to reach its destination will be higher. On an average it is 19.9% higher than the proposed scheme without attackers. Since it efficiently detects the attackers in the network it is acceptable. Hence a secure identity based scheme is proposed with less overheads and better performance.

VI. CONCLUSION

An Efficient identity based scheme is proposed against Sybil attackers in wireless sensor networks. Expensive pairing operations are not used in this scheme to reduce overheads. It provides authentication, message integrity and unlinkability. The proposed scheme is evidenced to be unforgeable under random oracle. The performance of the proposed scheme is analyzed by comparing its computation cost of message signing and aggregate verification with other schemes. It is shown that the proposed scheme has less computation overhead. Simulation results show that the proposed scheme has better performance in terms of PDR and delay even in the presence of Sybil attackers.

REFERENCES

1. J. Newsome, E.Shi, D.Song and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," ACM Journal, April 2004.
2. L. Lazos and R. Poovendran, ``SeRLoc: Secure range-independent localization for wireless sensor networks," in Proc. 3rd ACMWorkshop Wireless Secur., 2004, pp. 21_30.
3. L. Lazos and R. Poovendran, ``HiRLoc: High-resolution robust localization for wireless sensor networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 233_246, Feb. 2006.
4. M. Demirbas and Y. Song, ``An RSSI-based scheme for Sybil attack detection in wireless sensor networks," in Proc. Int. Symp. World Wireless, Mobile Multimedia Netw., 2006, pp. 564_570.
5. M. Wen, H. Li, Y.-F. Zheng, and K.-F. Chen, ``Tdoa-based sybil attack detection scheme for wireless sensor networks," J. Shanghai Univ. English Ed., vol. 12, no. 2, pp. 66_70, 2008.
6. Y. Zhang, K. F. Fan, S. Zhang, and W. Mo, ``AOA based trust evaluation scheme for Sybil attack detection in WSN," Appl. Res. Comput, vol. 27, no. 2, pp. 1847_1849, 2010.
7. X. Wang, L. Qian, and H. Jiang, ``Tolerant majority-colluding attacks for secure localization in wireless sensor networks," in Proc. 5th Int. Conf. Wireless Commun., Netw. Mobile Comput. (WiCom), Sep. 2009, pp. 1_5.

8. Y.Yuan, L. Huo, Z.Wang and D. Hogrefe, "Secure APIT Localization Scheme Against Sybil Attacks in Distributed Wireless Sensor Networks", IEEE Access, vol. 6, 2018, pp. 27629-27636.
9. G. Zhan, W.Shi and J. Deng, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs",IEEE transaction on dependable and secure computing, vol.9, no. 2, April 2012, pp.184-197.
10. H. Xiong, Z. Guan, Z. Chen, and F. Li, "An efficient certificateless aggregate signature with constant pairings computations," Inf. Sci., vol. 219, pp. 225-235, Jun. 2013.
11. J. Li, H. Yuan, and Y. Zhang, "Cryptanalysis and improvement for certificateless aggregate signature," Fund. Inf., vol. 157, nos. 1-2, pp. 111-123, Jan. 2018.
12. S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, and M. K. Khan, "An efficient certificateless aggregate signature with conditional privacypreserving for vehicular sensor networks," Inf. Sci., vol. 317, pp. 48-66, Oct. 2015.
13. J. Cui, J. Zhang, H. Zhong, R. Shi, and Y. Xu, "An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks," Inf. Sci., vols. 451-452, pp. 1-15, Jun. 2018.
14. Y. Qu and Q. Mu, "An efficient certificateless aggregate signature without pairing," Int. J. Electron. Secur. Digit. Forensics, vol. 10, no. 2, pp. 188-203, Apr. 2018.
15. P. Kumar, S. Kumari, V. Sharma, A. K. Sangaiah, J. Wei, and X. Li, "A certificateless aggregate signature scheme for healthcare wireless sensor network," Sustain. Comput., Inform. Syst., vol. 18, pp. 80-89, Jun. 2018.
16. L. Wu, Z. Xu, D. He, and X. Wang, "New certificateless aggregate signature scheme for healthcare multimedia social network on cloud environment," Secur. Commun. Netw., vol. 2018, Jun. 2018, Art. no. 2595273.
17. H. Du, Q. Wen, S. Zhang, "An Efficient Certificateless Aggregate Signature Scheme Without Pairings for Healthcare Wireless Sensor Network," IEEE Access, vol.7. 2019, April 2019, pp. 42683-42693.
18. Jenefa, J. & Mary Anita, E.A., "Secure Vehicular Communication Using ID Based Signature Scheme", Wireless Pers Commun vol. 98, no. 1, Jan 2018, pp. 1383-1411.
19. Jenefa, J. & Mary Anita, E.A., "An Enhanced Secure Authentication Scheme for Vehicular Ad Hoc Networks Without Pairings", Wireless Pers Commun, vol. 106, no. 2, May 2019. pp. 535-554.
20. E.A. Mary Anita, "Sybil Secure Architecture for Multicast Routing Protocols for MANETs", Communications in Computer and Information Science, Springer-Verlag GmbH Berlin Heidelberg, Volume 190, 2011, pp 111-118.