Computers, Materials & Continua
DOI:10.32604/cmc.2021.014643
Article

Tech Science Press

Secure Localization Based Authentication (SLA) Strategy for Data Integrity in WNS

V. Manikandan[1,*], M. Sivaram[1], Amin Salih Mohammed[2], V. Porkodi[3] and K. Shankar[4]

[1]Assistant Professor Research, Research Center, Lebanese French University, Erbil, 44001, Iraq
[2]Vice President, Lebanese French University, Erbil, 44001, Iraq
[3]Department of Information Technology, College of Engineering and Computer Science, Lebanese French University, Erbil, 44001, Iraq
[4]Department of Computer Applications, Alagappa University, Karaikudi, 630003, India
[*]Corresponding Author: V. Manikandan. Email: v.manikandan@lfu.edu.krd; vmanikandanme@gmail.com
Received: 05 October 2020; Accepted: 10 November 2020

Abstract: Wireless Sensor Networks (WSN) has been extensively utilized as a communication model in Internet of Things (IoT). As well, to offer service, numerous IoT based applications need effective transmission over unstable locations. To ensure reliability, prevailing investigations exploit multiple candidate forwarders over geographic opportunistic routing in WSNs. Moreover, these models are affected by crucial denial of service (DoS) attacks, where huge amount of invalid data are delivered intentionally to the receivers to disturb the functionality of WSNs. Here, secure localization based authentication (SLA) is presented to fight against DoS attack, and to fulfil the need of reliability and authentication. By examining state information, SLA projects a trust model to enhance efficacy of data delivery. Indeed, of the prevailing opportunistic protocols, SLA guarantees data integrity by modelling a trust based authentication, providing protection against DoS attackers and diminishing computational costs. Specifically, this model acts as a verification strategy to accelerate? attackers and to handle isolation. This strategy helps SLA in eliminating duplicate transmission and by continuous verification that results from conventional opportunistic routing. Simulation is performed in a MATLAB environment that offers authentic and reliable delivery by consuming approximately 50% of the cost in contrast to other approaches. The anticipated model shows better trade off in comparison to the prevailing ones.

Keywords: Wireless sensor networks; opportunistic routing; secure localization based authentication; denial of service; computational cost

1 Introduction

Wireless sensor networks have shown its progression in Internet of Things (IoT) field and act as a significant role to offer an extensive range application via sensors, like traffic management, smart home and grids for monitoring environment. WSN comprises certain sinks or receivers and huge amount of SNs that collectively gathers data to carry out diverse functionality [1].

Construct a WSN model that offers reliable delivery expected in IoT applications. Samples of these applications are smart healthcare are utilized for monitoring purposes, treating and tracking patients [2]. Here, SNs accumulate patients' physical data and propagate it to doctors' location [3]. Owing to this collected data, precision may be aware of patients' physiological status and it possesses an ability to produce appropriate diagnosis in appropriate time [4].

The above mentioned application needs to offer reliable transmission, measured as crucial parameter for successful prediction [5]. Moreover, with respect to changing and wireless medium, these are vulnerable to link failures because of signal fading or signal interference, which may drastically, reduces Quality of Service (QoS) [6]. Henceforth, providing effectual data delivery turns to be a challenging crisis in reliability of WSN data delivery. Moreover, preserving route for data flow with superior communication for wireless channels unsteadiness [7]. Moreover, as packets are broadcasted over multiple paths to receiver, effectual transmission and interferences are initiated that leads to added transmission failures.

At present, an effectual model to fulfil reliability is utilizing location based opportunistic routing that describes routing path prior to data transmission [8]. With transmission and shared characteristic of wireless channel, it facilitates packet transmission that should overhear multiple SNs. Indeed of single forwarder in conventional routing, numerous candidate forwarders are chosen in routing, that is placed owing to priorities described by sender of packet [9]. Henceforth, packet transmission is not disturbed till candidate that relays productively over it. In contrast to multi-path routing, it has superior recital due to its reduced transmission contentions or interferences among candidates [10].

One amongst conventional routing protocols; geographic is more attractive because of dynamic links, as it will not require maintaining or preserving paths from source nodes to sink. Henceforth, combination of opportunistic and geographic routing is specified to opportunistic model. Prevailing models can acquire higher consistency over inks. Moreover, they are influenced by severe DoS, where malicious attackers are gradually transmit huge amount of invalid data with illegal signatures, attempting to misuse resources and disturb functionality. Specifically, routing magnifies DoS attacks as the invalid data that are delivered to receiver with candidate forwarders that is intensified by theoretical examination and analysis results in further part of the work [11]. To fight against those attacks, an effectual location based security authentication model is essential, which will ensure that packets are transmitted from SNs, and are not modified by attackers in transmission process. Moreover, this provided numerous issues.

Initially, with prevailing digital signature may enormously raise cost of SN and enlarges data delivery delay [12]. SNs are generally energy constrained and with higher computational cost. Previous work has demonstrated that validation of one signature requires approximately of 1 s on MICAz and MICA2. Validation of each incoming packet on SN may exhaust resources quickly [13]. Henceforth, a novel lightweight authentication model to DoS attackers is most essential. Subsequently, data packet verification may break down candidate forwarders priority described by opportunistic routing, as verification delay is extremely much superior than data packets based time transmission [14]. Moreover, restoring candidate forwarders priority has to acquire reliability and integrity of data, which is an ultimate objective of the work. Thirdly, invalid data or constant verification over duplicate transmission is fulfilled by OR [15]. For instance, if initial candidate falls over invalid packet after verification, subsequently candidate cannot verify whether packets are dropped due to link failure or invalid function. It skips verification process and continues to deliver invalid packet as in Fig. 1 Conversely, it may carry out

similar verification process and drops it. Henceforth, a strategy for sharing verification information amongst candidates has to be designed to reduce incurred overhead.

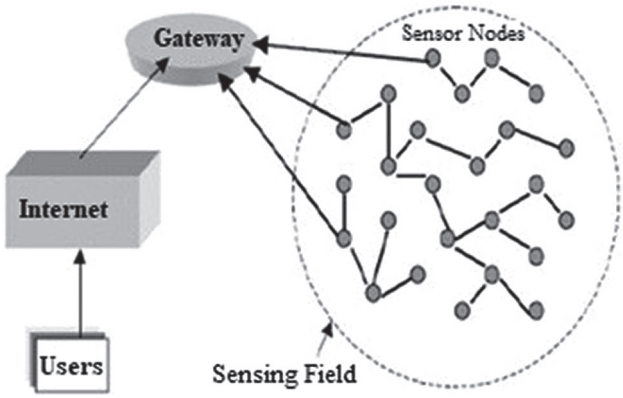

Figure 1: WSN network architecture

In this work, a secure localization based authentication strategy (SLA) is anticipated to fight against DoS attacks in WSNs for effectual location identification of nodes in dense environment. SLA attempts to guarantee reliability and authenticity of data packets for IoT based application. To enhance data delivery efficiency, SLA examines state information of nodes in wireless links, and constructs a trust based model for development of trust based localization approach for authentication. As well, SLA improves location based selective authentication includes 'verification' and 'warning'. Verification process is used to restore priorities of candidate forwarders in performing opportunistic routing. Warning notice process is used to share invalid signature for validating information amongst candidates, which has to accelerate attacker isolation. Accordingly, forwarders are permitted to withdraw redundant signature verification and duplicate data transmission. Extensive comparison depicts that the anticipated SLA can block up to 80% of invalid data with lower communication overhead that saves 50% of bandwidth and 50% of computation in contrast to other strategy.

Based on previous analysis, the anticipated model attempts to offer an effectual and reliable delivery while significantly preserves appropriate authentic data. Significant contribution is summarized as below:

1. Design of a standard trust model as a bottom line of modelling secure location based authentication to enhance stability and reliability of data delivery.
2. The source of DoS attack has been identified which shows severe security to WSN routing. Specifically, secure localization algorithm are initiated to isolate DoS with lesser cost.
3. Distributive verification strategy is anticipated exclusively to integrate authentication approach with opportunistic routing, while it drastically diminishes transmission of invalid data and signature verification provided by OR.
4. Theoretical analysis is performed to illustrate SLA effectually to fight against DoS attack; It is moderately reliable over unstable location of nodes and stability towards computational cost and communication resources.

Rest of the work is structured as follows: Section 2 explains in detail about background works. Section 3 depicts existing work on authentication process. Section 3 explains the security

and network model along with proposed idea. Section 4 provides a detailed outline of simulation results attained and analysis associated with it. Section 5 provides conclusion and future direction of research extension.

2 Related Works

In [16], Dini anticipated an ECC model that is considered as a well-equipped model. Moreover, based on the flaws encountered, such as, invalid presentation of mutual authentication amongst sensor and user, this scheme is considered to be insecure [17]. To improve and validate this process, Sun et al. [18] illustrated an enhanced version of this scheme which attempts to fight with security attributes and carry out reduced cost computation and communication overhead. Moreover, in [19] examined a strategy and proves that this model is faulty because of its lost or stolen smartcard attack, exhaustive sensor energy attack and key share attack. Indeed of corrective measures, Choi et al. [20] offered improved authentication protocol. In [21] provided public key version with ECC was anticipated so as to effectually deal with untraceability and carry out forward security.

In Perrig et al. [22] the author anticipated that the model is faulty and it cannot be handled with effectual security characteristics like insider attack, mutual authentication, user anonymity, session key agreement and pass-word guessing attack. In [23], author illustrated security characteristics effectually however they cannot be proven faulty like offline guessing attack, user anonymity attack, de-synchronization, forgery attack and lack of forward security strongly. As a solution, Wu illustrates a strategy with verification that is validating to improve security of WSNs.

In current improvements, So et al. [24] anticipated a strategy with symmetric cryptosystem. For validation, they maintain the ability to stand for diverse attack variants. Moreover, after investigation and analysis is mode in this scheme Cano et al. [25] proves the fault in Chen modelled not pass to resist over smart card loss attack, and DoS owing to inefficient verification approach. As well, Chen strategy is not successful to offer user anonymity as to verify user is broadcasted in plaintext constructed with login request. However, owing to delay in identifying inappropriate login credentials like password, Vettrile et al. [26] strategy misuse resources of user and as well SNs in both computational overheads and communication costs.

3 Proposed Work

3.1 Network Model

In this work, we consider a multi-hop WSN which comprises number of SNs and certain receivers or sinks which is deployed for some applications in IoT [27]. SNs lie in certain range in wireless transmission that could directly transmit data to one another. Multi-hop is facilitated with Euclidian distance is superior to transmission range. Consider sensor network in dense environment, where every sensor node possess enormous neighbourhood node [28]. Therefore, this network is depicted with graph G (V, L), where 'V' shows some set of SNs and 'L' shows direct link set amongst SNs as in Fig. 2. The link between nodes are defined when Euclidian distance amongst sensor node and receiver node is lesser than transmission of wireless range 'R'.

Consider that SNs are stationary, and they knew sink's position and location information. Indeed, nodes may generally aware of location information with neighbourhood nodes via beacons in common geographical routing, that is, SNs are transmitted with its identity periodically, residual energy and location information in beacons. As energy crisis is a major confront, consider sinks

are equipped with resourceful nodes and SNs that works on restricted batteries. Based on beacon messages, it is consistent to acquire energy information of neighbourhood nodes.

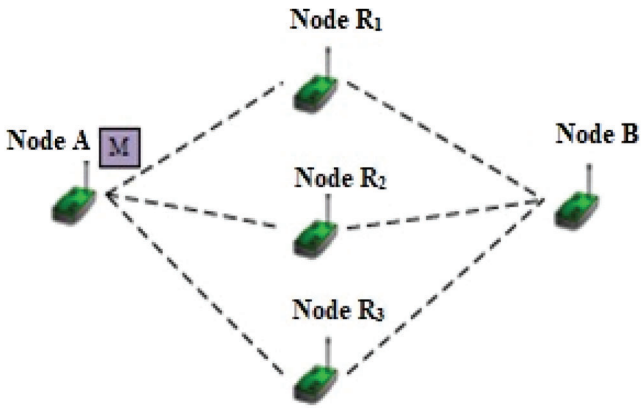

Figure 2: Network model

Here, we specifically spotlights on data delivery in network layer. To attain candidate forwarders co-ordination in this protocol, we study modified MAC protocol of anticipated OR sourced on ACK/RTS/CTS scheme in IEEE 802.11b. Moreover, MAC layer crisis like collision avoidance or hidden terminal is not determined in this work.

For security concern, Public Key Infrastructure is essential for key management. Assume every SN possesses key pair termed as: public and private key for verification and data packets. Trusted Certificate Authority (TCA) assists public keys as legal identities. In real time deployment, sinks or application developers plays TCA role. Consider that every sensor node recognizes knew public keys of node, and realizes private key to subsequent party.

3.2 Security Model

Here, the ultimate objective is to model an effectual and reliable delivery protocol that precisely preserves appropriate authentic data in WSNs [29]. Henceforth, essential properties of data packets has to be maintained.

3.2.1 Data Integrity

Prior to broadcasting packets, SNs has to assist to ensure data authenticity with neighbourhood nodes. Else, sinks has to receive enormous amount of data that disturb normal functionality. To offer data integrity to data packets, an authentication is crucial.

3.2.2 Non-Repudiation

Non-repudiation generally in co-operates authentication. It facilitates sink to validate third parties as sender is accountable for packet [30]. Here, sink may determine sender with invalid report attackers and packet to trust CAs.

3.2.3 Data Reliability

Due to the shared and broadcasting wireless medium, packets are vulnerable to drop for failures. However, data loss cause is extremely inevitable; it does not dissolve application

functionality that works based on IoT. Henceforth, it is needed to ensure superior reliability for delivery protocol.

3.2.4 Attacks Resistant

Devoid of authentication strategy, DoS transmit enormous invalid packets to dissolve communication network resources or disturb data delivery. However, SNs usually possess restricted energy and computational resources. To fight DoS, authentication mechanism possess low computational cost for energy efficiency.

3.3 Secure Localization Based Authentication Strategy

In this section, a secure localization based authentication strategy is anticipated along with its corresponding primary components.

3.3.1 Protocol Overview

The anticipated SLA protocol significantly comprises of three major elements: trust based mechanism, secure localization and authentication algorithm and verification scheme. Fig. 3 depicts the overview of proposed components as given below:

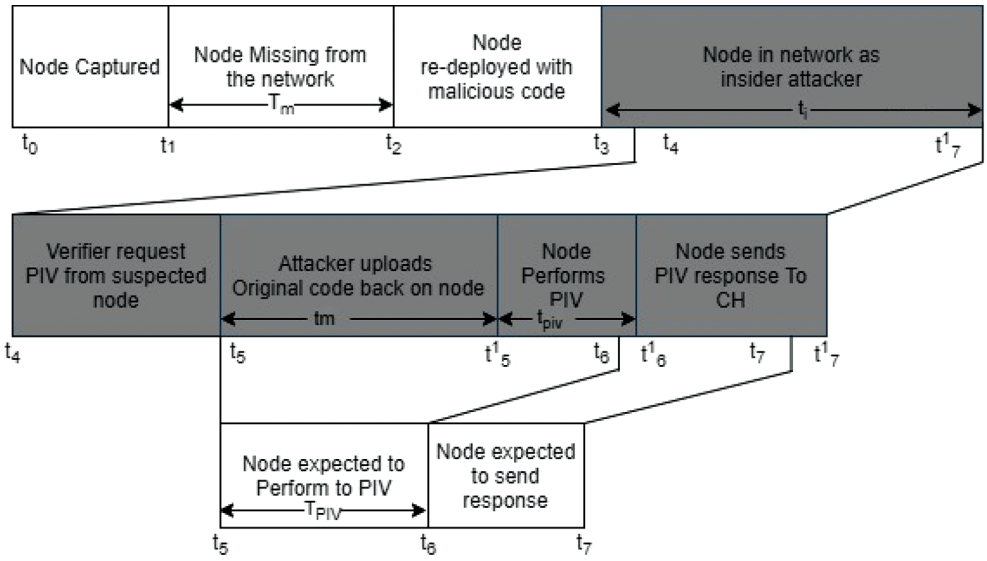

Figure 3: Timeslot of network

3.3.2 Trust Based Mechanism

By analyzing and collecting prevailing data transmission of wireless links, SNs provides state information of trusted model and updates dynamically the node state in WSNs. When data packets are received by receiver at sensor node, SNs has to demonstrate candidate forwarder set from neighbourhood so as to acquire reliable delivery in localization algorithm. To perform this, SNs has to allocate precedence to every candidate forwarder sourced on routing metrics depicted over state information based trust model. Henceforth, trust based mechanism comprises of state trust model, candidate forwarders and localization of nodes. The algorithm of the anticipated model is provided as below:

Algorithm 1: SLA mechanism

Input: data packets to be transmitted with highest priority
Output: successful delivery
If node ϵ C then
    Attaining data packet
        Start timer (t) based on nodes priority
End if
If timer (t) == 0 then
    Node turns to be hop sender and transmission
    Return
End if
While timer (t not equal to 0) do
If node overhears packet transmitted to another candidate node then
    Terminate timer (t)
Return
Endif
End while
    Node becomes hop sender is ready for transmission
Return

3.3.3 Selective Location Authentication

Before transmitting any data packets, SNs has to guarantee packet authenticity of packet to fight against DoS attacks. Localization dependent selective authentication mechanism is rapidly invalid packets devoid of validating signatures over hop. If sensor nodes knew less or abundant information regarding received signature, it is validated with superior or effectual probability. As well, node validation probability is leveraged, which could appropriately handle those received invalid signatures, to acquire attacker's isolation.

3.3.4 Verification Notice Strategy

When SN commences to validate data packet before transmission, it has to analyze candidate forwarders priority which is determined by anticipated routing. Therefore, a verification notice mechanism is designed to resolve these issues. After validation, warning notes mechanism is generated to share validation outcome amongst candidate forwarders for quicker isolation and efficiency. Verification notice strategy comprises of verification and warning notes as provided in algorithm.

Algorithm: Verification strategy

If node belongs to C, it becomes hop sender then
    Carry out authentication with output flag
If flag specifies verification then
    Transmit packet for verification note
        Verify packets

(Continued)

```
    If packets is invalid then
        Improve verification probability
            Transmit packet for warning notice
                Eliminate data packet
Else
        Transmit packet with SLA
End if
Else
        Transmit packet with SLA
End if
Else
        If node acquires verification then
        Improve timer
End if
If node receives warning message then
        Improve verification probability
        Stop timer and drop packet
End if
End if
```

3.3.5 Secure Localization Based Authentication Strategy

As discussed in previous sections, this SLA scheme comprises of four steps: Beacon exchange, Path testing, data aggregation along with location computation. LSA based authentication is performed in step two, that is, in testing phase. In testing, as anchor nodes triangle is chosen, every pair of anchor node chosen will be validated with signal strength. Receiver Signal Strength of SNs acquired from ith and jth anchor node correspondingly. The nodes threshold is defined as V-D. If $S = 1$, anchor 'i' and 'j' are suspect. Else, it is not suspect.

If two SNs are utilized as trustable to verify DoS attacks, certain legitimate nodes have to validate as DoS. An instance is provided in Fig. 3. 'A' and 'B' are two SNs, and 'X' and 'Y' are two legitimate anchor. If 'X' and 'Y' are exactly located over cross points of two network connectivity. Circle centre is 'A' and centre of connectivity is 'B'. Network connectivity radius is considered as distance amongst 'X' and 'A', while other is distance amongst 'B' and 'Y'. Here, legitimate nodes 'X' and 'Y' are considered as DoS nodes which are acquired from above scenario. If DoS attack is chosen inside triangle, this situation is considered in next step.

In this segment, an instance is provided to explain the process in detail:

Lemma 1: Anchor nodes like 'A', 'B', 'C' transmits a 'Hello Message' initially. After acquiring beacon from anchor nodes, SNs has to construct neighbourhood anchor table (Location, Receiver Signal Strength and Anchor ID), such as node 'X' and 'Y' with neighbourhood table correspondingly.

Lemma 2: After exchanging the corresponding neighbourhood table, SNs acquires the merged receiver anchor node information correspondingly.

Lemma 3: Authentication performed from selecting one triangle from nodes' table for instance, ABD. Anchor node such as (A, B) (B, C) (A, C) works over nodes column to validate DoS attack. If (A, B) anchor nodes are validated by SNs and outcomes are S = 1, anchor 'A' and 'B' are DoS.

Subsequent step is not performed over triangle. If (A, B) (B, C) (A, C) are superior anchor nodes, authentication is performed over each column of nodes table to validate receiver signal strength of neighbouring SNs. If there exist no neighbouring node that comprises of constant small or large RSS from A, B and C, then 'X' is ABC outside. Else, 'X' is inside.

Lemma 4: Lemma 3 is considered for repetition to iterate combinations of three anchor nodes.

Lemma 5: For all iterations are completed, area with reduced overlap may be considered and localization evaluation is in centre of gravity.

Algorithm 2: DoS attacker authentication

Input: 'S' and 'a'
For all anchor node do
    Transmit 'Hello' message
End
For all SNs do
    Construct receiver based neighbourhood anchor list
End
For all SNs do
    Integrate receiver anchor list from neighbour
    Construct SNs based on anchor list
End
For all anchor do
    For every pair of anchor from diverse column of integrated node list do
If DoS pair encountered do
    Count detection co-efficient
End
End
If $S > 3$ then
    Both anchor are DoS
    Eliminate them and transmit
        Continue
End
If SLA == out then
Add negative value
End
If SLA == In then
    Add positive value
End
End
Find region with maximum values
Evaluate localization of SNs with ROI region
Output: Localized SNs.

4 Numerical Results and Discussions

The simulation was carried out in a region of 300∗300 m. Here, SNs and anchor communication range is 65 and 125 m correspondingly. Anchor ratio to SNs is 1 to 10. One malicious node has to produce two DoS attacks by randomly determining location or ID of both of them. The anticipated model is iterated for 30 times to acquire optimal outcomes in Fig. 4. All executions are carried out on Lenovo G50 laptop, with Inter (R) Core i3 with CPU at 2.60 GHz and 6GB of RAM. Simulation setup was considered in MATLAB R2014a.

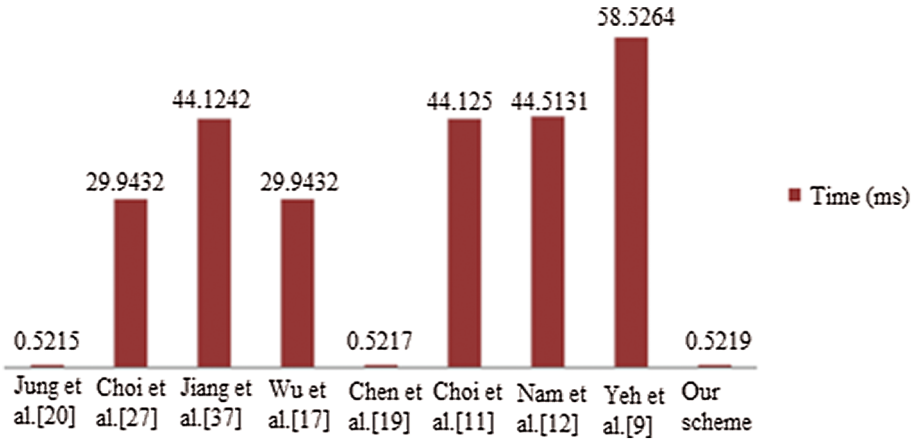

Figure 4: Computational cost

4.1 Average Detection Rate

This parameter depicts the average DoS detection of diverse amount of legitimate nodes (10–30), when DoS attack rose from 3 to 17. It is obvious to consider number of DoS attack raises, DoS will be predicted as in Fig. 5 Legitimate node is of larger size, then detection rate is also higher. This is due to the cause that no legitimate nodes are surrounded DoS decreases with increased legitimate node. Therefore, detection rate of 25 legitimate nodes can acquire more than 90%.

4.2 Average Localization Rate

Estimation of localization varies with number of beacon or anchor nodes. Number of DoS attack is 5 and number of legitimate anchor nodes rises from 15–35. Three diverse scenarios are considered here. The figure depicts the DoS scenario without DoS attack. Subsequent scenario is provided in red line that possesses DoS attacks, however devoid of detection strategy. It is observed that with sum of legitimate anchor nodes rises, localization estimation reduces. Rate of localization estimation of SLA model acquires 0.50R on average while there is no DoS attack is there. When SLA approach is influenced by DoS attack, average localization increases from 0.70R. SLA eliminates DoS attack in SLA and average localization is 0.45R, which improves localization based authentication accuracy.

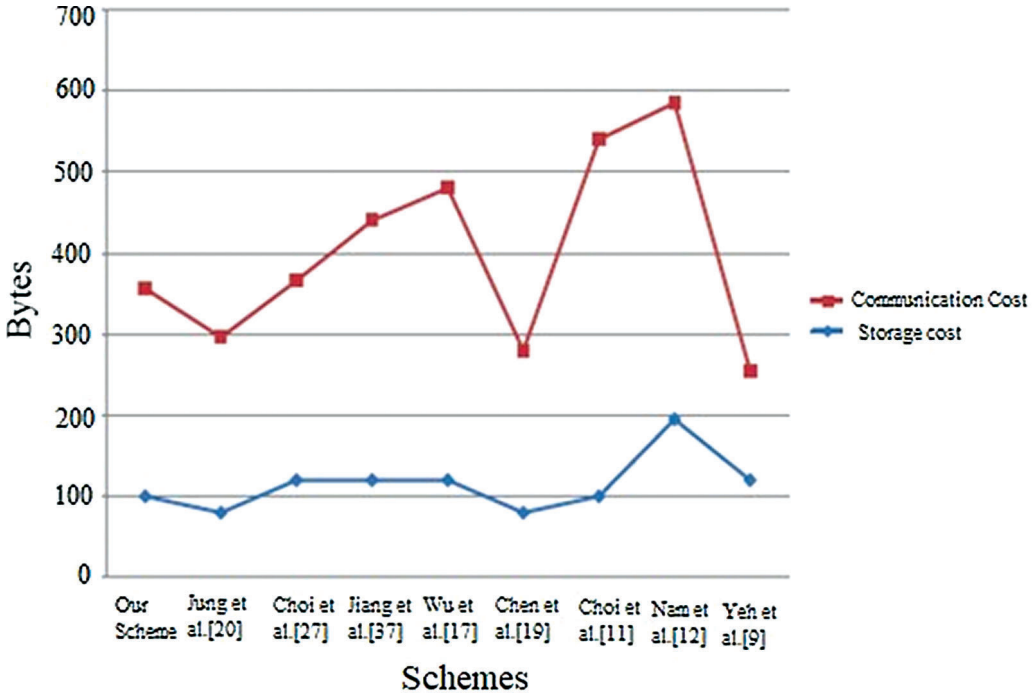

Figure 5: DoS detection rate based on communication cost and storage cost

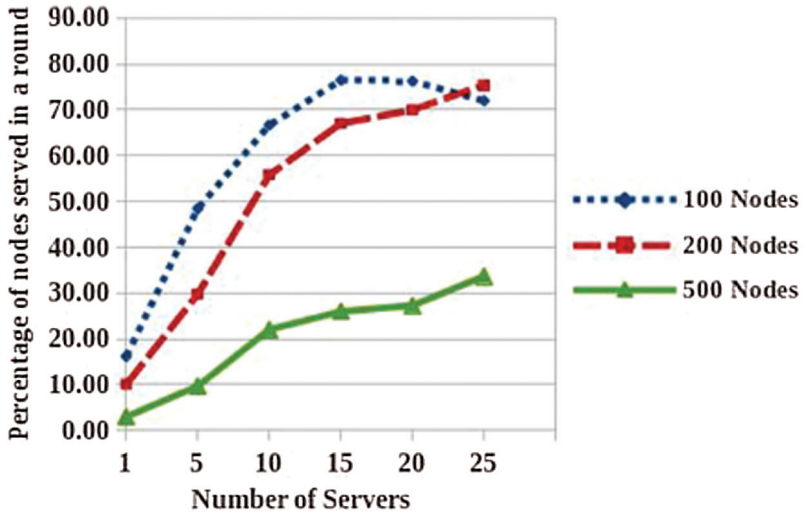

Figure 6: Nodes link quality based on servers

4.3 Nodes Link Quality

The performance of SLA with diverse in Fig. 6 link qualities is roughly about 60 network node, and evaluate it with three diverse scenarios: single path routing (for instance: GPRS), opportunistic routing (for instance: SLA) and opportunistic routing with authentication (for instance: SLA with trust model). For evaluation, this work introduces a novel SLA based trust mechanism

and localization algorithm, however it lacks in localization verification strategy. Node verification probability is 0.1. Link quality is packet reception ratio of wireless link from 0.2 to 1.

5 Conclusion

In this investigation, a novel Secure localization based authentication approach is anticipated, which tries to offer authenticity property and data delivery reliability for IoT applications. SLA exploits a state information based trust model to enhance reliability of delivery. To handle DoS attack, this work studied the prevailing authentication strategy and determined that they are failed to function over an opportunistic routing owing to its un-serviceability or high computational cost. Therefore, a novel trust based authentication model is isolated for DoS with reduced computational cost. To integrate localization based authentication algorithm with OR, we modelled distributive verification notice model, which can restricts invalid packets propagation and diminish sum of verification raised due to OR. Simulation setup shows that the anticipated model provides higher PDR even in poor links. With reduced communication cost, this method effectually eliminates DoS, thus significantly decreases computational cost in contrast to other model. From evaluation outcomes, the protocol works efficiently in terms of communication resources and computational cost. Moreover, end-to-end delay is considerably longer when superior node verification probability is identified. In future, the formulated problem has to deal with formulated problem and to adjust node verification probability to acquire optimal performance during delay. This work has to establish DoS behavioural model and examine enhancement in SLA.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Srinivas, A. K. Das, M. Wazid and N. Kumar, "Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial internet of things," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, pp. 1–7, 2018.

[2] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu *et al.,* "Secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," *Journal of Supercomputing*, vol. 74, no. 12, pp. 1–26, 2017.

[3] S. Kumari, "Design flaws of an anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography," *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13581–13583, 2016.

[4] F. Wu, L. Xu, S. Kumari and X. Li, "An improved and provably secure three-factor user authentication scheme for wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 11, no. 1, pp. 1–20, 2018.

[5] S. Kumari, L. Xiong, W. Fan, D. Ashok Kumar, A. Hamed *et al.,* "A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps," *Future Generation Computer Systems*, vol. 63, no. 1, pp. 56–75, 2016.

[6] C. Sravani, D. Ashok Kumar, O. Vanga, K. Neeraj, S. Kumari *et al.,* "An efficient ECC-based provably secure three factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Computers & Electrical Engineering*, vol. 69, no. 6, pp. 534–554, 2018.

[7] F. Wu, L. Xu, S. Kumari and X. Li, "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on internet of things security," *Journal of Ambient Intelligence and Humanized Computing*, vol. 8, no. 1, pp. 101–116, 2018.

[8] L. Xiong, P. Jieyao, N. Jianwei, W. Fan, L. Junguo *et al.,* "A robust and energy efficient authentication protocol for industrial internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1606–1615, 2018.

[9] H. L. Yeh, T. H. Chen, P. C. Liu, T. H. Kim and H. W. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 11, no. 5, pp. 4767–4779, 2011.

[10] W. Cheng, J. Li and H. Li, "An improved APIT location algorithm for wireless sensor networks," *Springer*, vol. 139, pp. 113–119, 2012.

[11] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam *et al.,* "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 14, no. 6, pp. 10081–10106, 2014.

[12] J. Nam, M. Kim, J. Paik, Y. Lee and D. A. Won, "A provably-secure ECC based authentication scheme for wireless sensor networks," *Sensors*, vol. 14, no. 11, pp. 21023–21044, 2014.

[13] S. Li, S. Zhao, X. Wang, K. Zhang and L. Li, "Adaptive and secure load balancing routing protocol for service-oriented wireless sensor networks," *IEEE Systems Journal*, vol. 8, no. 3, pp. 858–867, 2014.

[14] J. Liu, Z. Wang, M. Yao and Z. Qiu, "VN-APIT: Virtual nodes-based range free APIT localization scheme for WSN," *Wireless Networks*, vol. 22, no. 3, pp. 867–878, 2016.

[15] T. Park and K. G. Shin, "Attack-tolerant localization via iterative verification of locations in sensor networks," *ACM Transactions on Embedded Computing Systems*, vol. 8, no. 1, pp. 2–16, 2008.

[16] P. Perazzo, L. Taponecco, A. A. D'amico and G. Dini, "Secure positioning in wireless sensor networks through enlargement miscontrol detection," *ACM Transactions on Sensor Networks*, vol. 12, no. 4, pp. 27–45, 2016.

[17] F. Wu, L. Xu, S. Kumari and X. Li, "A new and secure authentication scheme for wireless sensor networks with formal proof," *Peer-to-Peer Networking and Applications*, vol. 10, pp. 1–15, 2015.

[18] C. Sun, J. Liu, X. Xu and J. Ma, "A privacy-preserving mutual authentication resisting DoS attacks in vanets," *IEEE Access*, vol. 5, pp. 24012– 24022, 2017.

[19] L. Chen, F. Wei and C. Ma, "A secure user authentication scheme against smart-card loss attack for wireless sensor networks using symmetric key techniques," *International Journal of Distributed Sensor Networks*, vol. 11, no. 4, pp. 704502, 2015.

[20] J. Jung, J. Kim, Y. Choi and D. Won, "An anonymous user authentication and key agreement scheme based on a symmetric cryptosystem in wireless sensor networks," *Sensors*, vol. 16, no. 8, pp. 1299, 2016.

[21] N. Ristanovic, P. Papadimitratos, G. Theodorakopoulos, J. Hubaux and J. Le Boudec, "Adaptive message authentication for multi-hop networks," in *Int. Conf. on Wireless On-Demand Network Systems and Services*, Bardonecchia, Italy, pp. 96–103, 2011.

[22] A. Perrig, J. Stankovic and D. Wagner, "Security in wireless sensor networks," *Communication of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[23] D. He, C. Chen, S. Chan and J. Bu, "DiCode: DoS-resistant and distributed code dissemination in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 5, pp. 1946–1956, 2012.

[24] 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, 2017.

[25] 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, 2016.

[26] G. Schaefer, F. Ingelrest and M. Vetterli, "Potentials of opportunistic routing in energy-constrained wireless sensor networks," in *Proc. EWSN*, Cork, Ireland, pp. 11–13, 2009.

[27] Y. Choi, Y. Lee and D. Won, "Security improvement on biometric based authentication scheme for wireless sensor networks using fuzzy extraction," *International Journal of Distributed Sensor Networks*, vol. 2016, pp. 1–16, 2016.

[28] 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, 2014.

[29] M. Krotofil, A. A. Crdenas, B. Manning and J. N. Larsen, "CPS: Driving cyber-physical systems to unsafe operating conditions by timing DoS attacks on sensor signals," in *Proc. ACSAC*, New York, NY, USA, pp. 146–155, 2014.

[30] Q. Jiang, N. Kumar, J. Ma, J. Shen, D. He *et al.,* "A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks," *International Journal of Network Management*, vol. 27, no. 3, pp. 1–17, 2016.