Hindawi
Wireless Communications and Mobile Computing
Volume 2017, Article ID 8457616, 8 pages
https://doi.org/10.1155/2017/8457616

WILEY | Hindawi

Research Article

A Replica Detection Scheme Based on the Deviation in Distance Traveled Sliding Window for Wireless Sensor Networks

Alekha Kumar Mishra,[1] Asis Kumar Tripathy,[2] Arun Kumar,[3] and Ashok Kumar Turuk[4]

[1]*School of Computer Science and Engineering, VIT University, Tamil Nadu, India*
[2]*School of Information Technology and Engineering, VIT University, Tamil Nadu, India*
[3]*Department of Electrical & Computer Engineering, National University of Singapore, Singapore*
[4]*Department of Computer Science and Engineering, National Institute of Technology, Rourkela, India*

Correspondence should be addressed to Alekha Kumar Mishra; alekha.mishra@vit.ac.in

Received 29 July 2016; Accepted 24 October 2016; Published 15 January 2017

Academic Editor: Patrick Seeling

Node replication attack possesses a high level of threat in wireless sensor networks (WSNs) and it is severe when the sensors are mobile. A limited number of replica detection schemes in mobile WSNs (MWSNs) have been reported till date, where most of them are centralized in nature. The centralized detection schemes use time-location claims and the base station (BS) is solely responsible for detecting replica. Therefore, these schemes are prone to single point of failure. There is also additional communication overhead associated with sending time-location claims to the BS. A distributed detection mechanism is always a preferred solution to the above kind of problems due to significantly lower communication overhead than their counterparts. In this paper, we propose a distributed replica detection scheme for MWSNs. In this scheme, the deviation in the distance traveled by a node and its replica is recorded by the observer nodes. Every node is an observer node for some nodes in the network. Observers are responsible for maintaining a sliding window of recent time-distance broadcast of the nodes. A replica is detected by an observer based on the degree of violation computed from the deviations recorded using the time-distance sliding window. The analysis and simulation results show that the proposed scheme is able to achieve higher detection probability compared to distributed replica detection schemes such as Efficient Distributed Detection (EDD) and Multi-Time-Location Storage and Diffusion (MTLSD).

1. Introduction

Sensor networks have been a topic of interest among the academia and industry due to their wide range applicability in various network environments. WSNs consist of a large number of tiny sensors, usually deployed densely in the target area to collect relevant data [1, 2]. Sensor nodes are resource-constrained due to their small size and this limits the ability of computation and communication. The most common applications of WSNs include habitat monitoring, border patrolling in military, traffic monitoring, and patient monitoring in healthcare [3, 4].

In MWSNs [5, 6], sensor nodes have additional mobility function to wander inside a target area. Mobile sensor nodes can provide accurate data compared to static nodes. The number of sensors required in MWSNs for covering a given area is quite lesser than static WSNs. Nevertheless, dense deployment of mobile nodes supports high reliability and load balancing. Despite all advantages, MWSNs possess a highly dynamic network topology due to mobility. Therefore, the challenges are multiplied compared to their static counterparts. The major challenges include communication, coverage, distributive cooperative control, and security [7, 8]. Security has always been a critical issue of concern in WSNs [9]. Taking the advantage of flexibility in deployment, an outsider can launch attacks at various levels of communication layers in WSNs. The list of attacks of high threat includes wormhole, sinkhole, desynchronization, hello flooding, and Sybil [10]. Node replica attack is a serious attack and difficult to handle in WSNs [11]. In this attack, an adversary captures a node and deploys one or more replicas of it in the network. The aim behind such attack is to take control over the

network activities and launch insider attacks with the help of replicas. Therefore, detection of node replication attack should be done as early as possible. The replica detection schemes in MWSNs as reported in the literature are very few in numbers [12]. The schemes proposed by Ho et al. [13] and Deng et al. [14] rely on node's location claim to detect replica. In these schemes, the received location claims are used to compute the node's speed in the network. A replica is detected, when its speed exceeds the predefined maximum speed limit. However, in these schemes, BS performs the task of replica detection and therefore is exposed to single point of failure. These schemes also incur an additional communication overhead of sending node's location claim to the BS.

In this paper, we propose a distributed replica detection scheme for MWSNs that uses time-distance broadcast of nodes to detect a replica. The proposed detection scheme is based on the fact that when a node i and its replica coexist in the network, it would lead to deviation in the distance traveled by i at any instance of time. In the proposed scheme, every node performs the role of an observer node for a number of nodes in the network. Observers are responsible for maintaining a sliding window of recent time-distance broadcast of nodes under observation. When a deviation is detected in the distance traveled by a node, this is recorded by the observer nodes. The degree of violation of a node is computed from the recorded deviations. When the degree of violation of a node is measured above a predefined threshold, it is detected as replica. The threshold measured using simulation experiments. The proposed scheme is fully distributed and found to have higher detection probability and an average communication overhead compared to the existing schemes such as EDD and MTLSD.

The rest of the paper is organized as follows: Section 2 provides an overview of the existing node replica detection schemes. Assumptions about the adversary and network are enlisted in Section 3. The proposed scheme is explained in Section 4. Analysis of the proposed scheme is presented in Section 5. Simulation results are detailed in Section 6, and Section 7 summarizes the concluding remark.

2. Related Works

The detection schemes for static WSNs are not applicable to MWSNs due to dynamic network topology. A detection mechanism in MWSNs must take the mobility of a node into account in order to detect replica [15]. The replica detection mechanisms in MWSNs as reported in the literature are described below.

The detection schemes Unary-Time-Location Storage and Exchange (UTLSE) and Multi-Time-Location Storage and Diffusion (MTLSD) proposed by Deng et al. [14] adopt time-location claim approach. Each node in UTLSE and MTLSD stores multiple instances of time-location claim of the tracked nodes. On meeting, the time-location schemes are exchanged between two trackers to verify the feasibility of location claims. When a conflict arises in the time-location verification process of a node, it is detected as replica.

A detection scheme using node's speed is proposed by Ho et al. [13]. This scheme uses Sequential Probability Ratio Test to compute node's speed. When a node arrives at a new location, it broadcasts its time-location claim to the neighbors. Neighbors forward the received claim to BS after successfully verifying the authenticity of the message. The BS is responsible for gathering time-location claims of the nodes and measures their speed. A node with a speed higher than the predefined speed limit is detected as replica by the BS.

A pairwise key establishment process to detect existence of replica is presented by Deng and Xiong [16]. The total number of pairwise keys established by a node is stored using Counting Bloom filter. The count of number of keys established is periodically sent to the BS by each node. The received Counting Bloom filters are updated at BS for each node in the network. When the number of keys established for a node exceeds the predefined threshold value, the node is detected as replica by the BS.

A single-hop based replica detection scheme is proposed by Sindhuja and Padmavathi [17]. In their work, the witness node selection method of single-hop replica detection is improved by using clonal selection algorithm. The best suitable witness for a node in its single-hop neighbor is selected using the clonal selection algorithm. The neighborhood fingerprint sharing and verification method is used to detect replica.

The Extremely Efficient Detection (XED) and Efficient Distributed Detection (EDD) schemes are proposed by Yu et al. [18, 19]. The detection of replica in XED is based on the exchange of a random number between each pair of nodes, which is also called a challenge. When the same pair of nodes meet each other at a later point of time, the challenge verification is performed. A node that fails the challenge verification process is detected as a replica. In EDD, a replica is detected based on the count of number of meetings between a pair of nodes. If the number of meetings of a node over a time interval exceeds the predefined threshold, then it is detected as replica.

In the detection schemes by Ho et al. [13] and Deng and Xiong [16], the replicas are detected by the BS. In these schemes, BS is overburdened with computation and replica detection tasks. There is also an additional overhead in the network for communicating between all the nodes and the BS. The XED mechanism is not resilient to stealing of challenge from a captured node. In EDD scheme, the performance of detection mechanism depends on the number of meetings threshold, which is difficult to estimate in MWSNs. This is because the number of meetings with a node over a time interval depends on the network size, the area of deployment, node's speed, and the mobility model of the nodes. It changes with the variation of any of these parameters in the network. For example, if the network size is increased, then the number of meetings with a particular node decreases, as prob(meeting) $\propto$ 1/network size. Estimating a threshold on number of meetings with a node without considering the variation of the abovementioned parameters may result in false detection. In the scheme proposed by Deng et al. [14], the replica is detected solely based on a single case of conflict with the measured speed. The speed is computed

using the Euclidean distance between reported locations of a node over a time interval. This may not compute the actual speed of a node in the network with random waypoint mobility model. When a node moves faster by changing the direction frequently, it never follows a straight path. Moreover, since the locations of replica and the original node are used to measure the deviating speed, the adversary may deploy the replicas to move within closer premises of the original node to keep the measured speed within the accepted range. In the scheme proposed by Sindhuja and Padmavathi [17], the neighborhood fingerprint mechanism is not suitable for MWSN, due to the dynamic topology of the network. Moreover, selection of a single witness node may lead to a low replica detection probability, where the neighboring nodes are frequently changing over time. The replica detection process should not decide based on one time conflicting behavior of a node and its replica while using the parameters, such as speed and number of meetings, but rather behavior should be observed over a number of time intervals. In the proposed work, the detection process makes decision based on the observation of the behavior of a node over a number of time intervals.

3. Assumptions

The assumptions for the proposed scheme are enlisted below. The network assumptions are presented in Section 3.1, and assumptions regarding adversary are presented in Section 3.2.

3.1. Assumptions about Network. The nodes in MWSNs are assumed to be homogeneous. Sensors are randomly deployed in the network and they follow random waypoint mobility model [20] for movement within the target area. Node's speed lies within the interval $[v_{\min}, v_{\max}]$, where $v_{\min}$ and $v_{\max}$ are the minimum and maximum speed, respectively. The communication among the nodes is bidirectional. A light-weight identity-based signature scheme [21, 22] is used for message authentication. All nodes are tightly synchronized with respect to time. It is also assumed that a node remains idle at a particular location for a period not more than predefined pause time.

3.2. Assumption about Adversary. An adversary is assumed to have the ability to compromise a subset of nodes in the network. It can create as many replicas of the captured node as it wishes and deploy them at various locations in the network. Adversary does not have the ability to generate new identity of a node. It is also assumed that it cannot predict the position and movement of a legitimate node because of random waypoint mobility model. Finally, an adversary also cannot predict the list of observers of a captured node and obeys all the communication protocols of the network.

4. Proposed Work

In this section, we discuss the proposed replica detection scheme for MWSNs. The proposed scheme is based on the following concept: "in MWSNs with random waypoint mobility model, the existence of one or more replicas of a node in the network contributes a significant deviation in the actual distance traveled by the node over a given time interval. This fact is recorded by the observer nodes and considered to obey a high degree of violation if the deviation persists over the period of observation." The proposed scheme is distributed in nature. In this scheme, each node performs the role of observer for a set of nodes in the network. Each observer maintains a sliding window of size w to keep track of recent distance traveled values at various time instances. The degree of violation is computed based on the frequency of the deviation recorded in the distance traveled by a node. A replica is detected by an observer, when the degree of violation of a node is higher than a specified threshold value. Section 4.1 explains the process of sharing the time-distance values by the nodes and updating the sliding window by the observers, and Section 4.2 details the process of replica detection.

4.1. Time-Distance Pair Sharing. Each node computes and maintains the distance traveled at the end of each epoch and locally broadcasts a time-distance pair at regular intervals. The format of the broadcast message from a node, say, A, is given below:

$$A \longrightarrow * : \left[A, T^A, D, \text{Signature}_A\right]. \tag{1}$$

Here, A is the identity of the node, T^A is the timestamp of A, D is the distance traveled by A at time T^A, and Signature_A is the signature, signed by A.

Let the node B be an observer of A. Node B maintains a sliding window W_A of size w containing recent time-distance broadcasts of A. Let $W_A = \{(d_i, t_i), (d_{i+1}, t_{i+1}), \ldots, (d_j, t_j)\}$, where (d_j, t_j) is the jth time-distance pair broadcast received by B from A, and $j > i$. Node B upon receiving a new time-distance pair from the node A verifies its signature and updates W_A by removing the earliest pair from it. For example, if $w = 10$ and $W_A = \{(d_5, t_5), (d_6, t_6), \ldots, (d_{15}, t_{15})\}$, then after receiving (d_{16}, t_{16}) from A the updated $W_A = \{(d_6, t_6), (d_7, t_7), \ldots, (d_{16}, t_{16})\}$. Every time the sliding window of an observer is updated, it measures the deviation and the degree of violation of the node to detect replica. The following section defines the degree of violation and describes the process of replica detection.

4.2. Replica Detection. When an adversary deploys replica of a captured node, say, C in the network, the replicas will compute distance traveled and broadcast it at regular interval, despite their other malicious activities. In this circumstance, one or more observers of C are going to detect either of the following conditions while updating W_C: for any pair of time-distance pair instances (d_j, t_j) and (d_k, t_k),

$$d_j \geq d_k \quad \text{if } t_j < t_k, \tag{2}$$

$$\frac{d_k - d_j}{t_k - t_j} \notin [v_{\min}, v_{\max}] \quad \text{if } t_j < t_k,\ d_j < d_k. \tag{3}$$

An observer marks the condition satisfied by either (2) or (3) as a deviation. This deviation of the node C is recorded

using a binary deviation array, D of size w. At the beginning of detection process, the D array of each node is set to zero. The deviation of a node C is updated using the following operations:

$$D_C \ll 1, \tag{4}$$

where $\ll$ is the left shift operation of bits,

$$D_C[w-1] = \begin{cases} 1 & \text{if deviation is marked} \\ 0 & \text{otherwise.} \end{cases} \tag{5}$$

Using D_C, the observers compute the degree of violation ($\deg V$) for C, which is defined by the following equation:

$$\deg V = k \cdot \frac{d_V}{n(d_V)}, \tag{6}$$

where d_V is given by

$$\begin{aligned} d_V &= \sum_{\substack{\forall p,q \\ \text{s.t } D_C[p]=D_C[q]=1}} \frac{1}{\sqrt{(p-q)^2}}, \\ n(d_V) &= \sum_{\substack{\forall p,q \\ \text{s.t } D_C[p]=D_C[q]=1}} . \end{aligned} \tag{7}$$

Here k is a constant. A node C is detected as replica when $\deg V$ is greater than a given threshold η. The value of η is assigned using a set of replica-deployment scenarios during the simulation.

5. Analysis

Claim 1. For any pair of time-distance broadcasts (d_j, t_j) and (d_k, t_k), either of the following conditions holds:

(I)

$$d_j \geq d_k \quad \text{if } t_j < t_k, \tag{8}$$

(II)

$$\frac{d_k - d_j}{t_k - t_j} \notin [v_{\min}, v_{\max}] \quad \text{if } t_j < t_k,\ d_j < d_k. \tag{9}$$

Proof. Here, we show that when an observer receives time-distance broadcast from a node and its replica, either of the above conditions holds true. Let us consider two nodes n_a and n_b moving in a rectangular target field of size $x \times y$. According to random waypoint mobility model, the node selects a target location and a speed at random from $[v_{\min}, v_{\max}]$ at the beginning of each epoch. Let the range of distance of an epoch be $[1, \sqrt{x^2 + y^2}]$. The distance traveled by a node and its replica will be the same for a given time interval only if the speed and target distance for all epochs are same. The probability of choosing a speed and distance by a node follows uniform distribution, that is, for a speed, $v \in [v_{\min}, v_{\max}]$, and an epoch distance, $d \in [1, \sqrt{x^2 + y^2}]$:

$$P(v, d) = \frac{1}{(v_{\max} - v_{\min}) \cdot \left(\sqrt{x^2 + y^2} - 1\right)}. \tag{10}$$

This probability is significantly small for even a small range of speed and distance. For example, the common speed range of mobile sensor is taken as [2,8] m/s, and a small target area size is $100 \times 100\ \text{m}^2$. Using these values in the above equation, the probability is given by

$$P(v, d) = \frac{1}{8 \times 140.4} \approx 0.0009. \tag{11}$$

Hence, the distance traveled by a node and its replica will never be same. Therefore, at any time t, $d_j \neq d_k$. Based on the broadcast time of the pair (d_j, t_j) and (d_k, t_k), either $d_j > d_k$ or $d_k > d_j$ will hold true. In case (II), the distance d_j is always received from a replica and d_k from the original node. This is because the replicas are deployed after the deployment of original node. In this case, the $d_j - d_k$ will be greater than the traveling limit of the nodes. Hence, in either case, the above conditions will hold true. □

5.1. Security Analysis. A malicious node may attempt to forge a time-distance pair. However, on receiving the time-distance broadcast, the node's identity and the signature are verified by the observers. Therefore, malicious node cannot forge time-distance broadcast. A node may skip the process of broadcasting time-distance pair. In this case, when observers do not get an update from a node over a longer period of time, they blacklist the node for violating security protocol. An adversary will not gain much benefit if replicas move together and stay close enough so that all could travel the same distance. This is because these nodes would essentially have the same set of neighbors and an observer would always receive a single time-distance broadcast from the same node at a time. An adversary may also modify replicas to broadcast a fake or manipulated time-distance pair that is close to the legitimate node. However, due to random waypoint mobility model, a node cannot predict the movement of another node in the network. In other words, a replica cannot guess the distance traveled by its legitimate node by any means. In this case, the intended replica would broadcast a random distance instead of the actual ones. As per the given conditions to measure the deviation, any random distance may lead to a deviation with a high probability and can be handled by an observer.

5.2. Communication and Storage Overhead. The communication in the proposed scheme involves local broadcast in the neighborhood. Therefore, the communication complexity of the proposed scheme for a network of size N is $O(N)$. The storage overhead of the proposed scheme depends on w. According to Birthday Paradox [23], $\sqrt{N}$ number of

Table 1: Comparison of communication and storage overhead.

Schemes	Type	Communication	Storage
UTLSE & MTLSD [14]	Distributed	$O(N)$	$O(\sqrt{N})$
Ho et al. [13]	Centralized	$O(N\sqrt{N})$	$O(N)$
Deng and Xiong [16]	Centralized	$O(N\sqrt{N})$	$O(k)$
XED [19]	Distributed	$O(1)$	$O(N)$
EDD [19]	Distributed	$O(1)$	$O(N)$
Proposed	Distributed	$O(N)$	$O(w\sqrt{N})$

Table 2: Simulation parameters.

Parameter	Value
Simulation area	$1000 \times 1000\ \text{m}^2$
Network size	100–1000 nodes
Deployment type	Uniformly random
Communication range	30 meter
Node movement	Random way-point mobility model
Node's speed	2–8 meters/sec
Simulation time	800 sec

observers is sufficient to detect replica with a high probability. Therefore, the storage overhead associated with a node in the proposed scheme is $O(w\sqrt{N})$, where $w \ll N$. The comparison of communication and storage overhead of the proposed scheme with the existing schemes is shown in Table 1.

5.3. Detection Probability. Detection of replica depends on the probability of successful reception of time-distance broadcast from a replica by an observer. Let r be the number of replicas deployed in the network, where $r \ll N$. Using Birthday Paradox [23], let $\sqrt{N}$ be the number of observers per node. Then, the probability of detecting a replica is expressed as the probability of meeting a replica by its observer. That is,

$$\begin{aligned} &P_{\text{repdet}} \\ &= P\ (\text{probability of meeting of a pair of nodes in the network, such that one of them is a replica, and other is its observer}) \\ &= \frac{r \cdot \sqrt{N}}{\binom{N}{2}} = \frac{2 \cdot r \cdot \sqrt{N}}{N(N-1)}. \end{aligned} \tag{12}$$

From the above equation, it can be inferred that the detection probability increases with the number of replicas and observers in the network.

6. Simulation and Results

The Castalia 3.2 [24] simulator is used for simulation of the proposed scheme in Omnet++ simulation environment [25]. An area of $1000 \times 1000\ \text{m}^2$ is considered for simulation, where nodes are uniformly deployed within the simulation area. The network size is varied from 100 to 1000 nodes during simulation. Nodes use random waypoint mobility model for movement. Replicas are randomly deployed by compromising multiple nodes. We observed during the simulation that the replica detection is high when η is 0.5. The summary of simulation environment parameters is provided in Table 2. The performance of the proposed scheme is evaluated using the following metrics: (i) detection probability, (ii) first replica detection time, (iii) number of packets sent/received, (iv) energy consumed per node, and (v) false detection rate. The proposed scheme is compared with two popular distributed replica detection mechanisms: MTLSD [14] and EDD [19].

Figure 1 shows the comparison of detection probability versus network size for number of replicas equal to 10. It is observed that proposed scheme has higher detection probability in comparison to EDD and MTLSD. This is because in the proposed scheme the deviation in distance traveled by the replica is successfully recorded and detected by its observer nodes. However, in the schemes EDD and MTLSD the replica detection relies upon the number of meetings with the nodes and the time-location claims exchanged between a pair of nodes, respectively. It is found that it is difficult to achieve higher detection probability by considering these parameters and as a result the detection probability is lower in these schemes.

The comparison of detection probability versus number of replicas for the network size of 500 is shown in Figure 2.

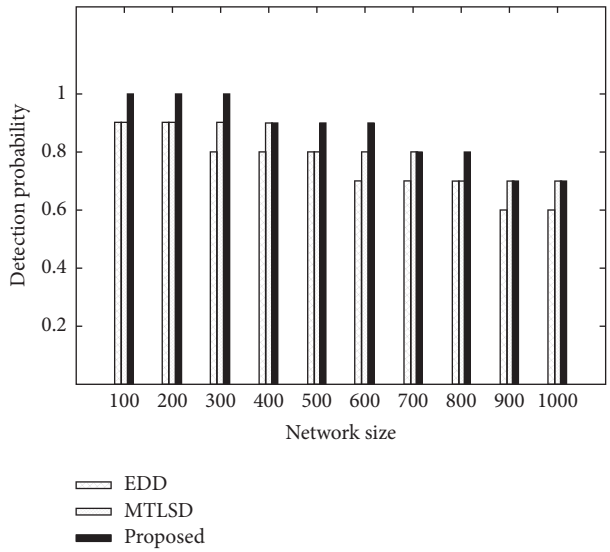

Figure 1: Comparison of detection probability versus network size for the number of replicas equal to ten.

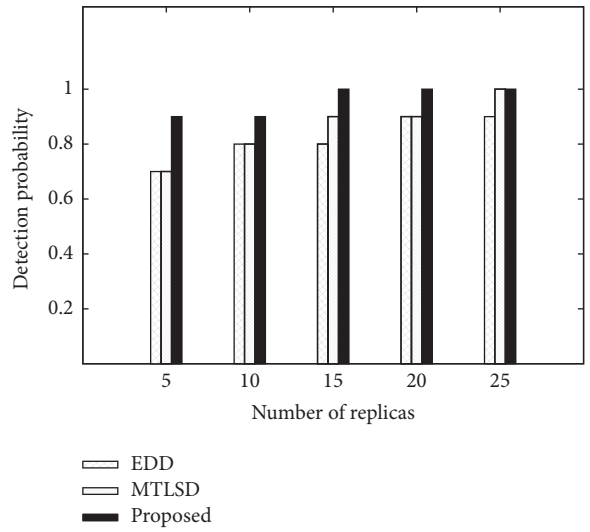

Figure 2: Comparison of detection probability versus number of replicas for $N = 500$.

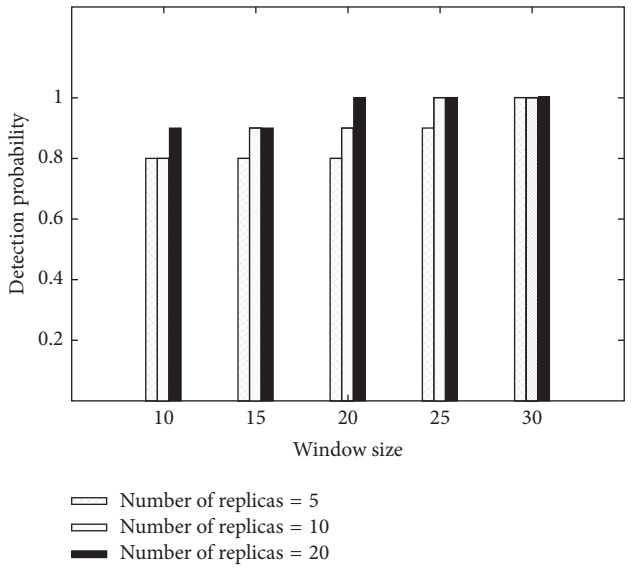

Figure 3: Comparison of detection probability versus window size for the number of replicas equal to ten and $N = 500$.

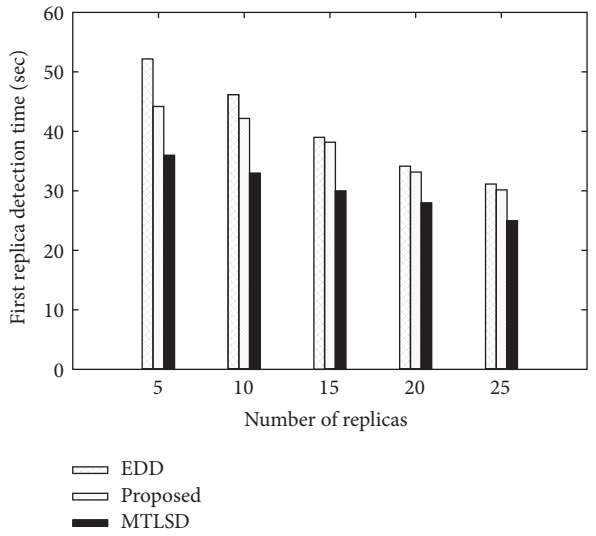

Figure 4: Comparison of detection time versus number of replicas deployed.

It is observed that the detection probability of proposed scheme increases with the number of replicas in the network. The increase in the number of replicas contributes to higher meeting probability of replica with its observer nodes. It is also observed that the detection probability of proposed scheme is higher than other schemes with different number of replicas. The sliding window size is one of the parameters that influence the efficiency of recording deviation. The plot for detection probability versus window size by varying the number of replicas is shown in Figure 3. It is observed that the detection probability is high when window size is 30. The detection probability remains unchanged, when the window size is greater than 30.

The plot for comparison of first replica detection time versus number of replicas deployed is shown in Figure 4. It is observed that the first replica detection time of the proposed scheme lies between EDD and MTLSD. This is because the detection of replica is done based on the degree of violation, which takes a marginally higher amount of time than time-distance claim diffusion process in MTLSD. EDD have higher detection time than the rest of the schemes, because EDD checks for number of meetings with other nodes over a predefined time interval and this takes relatively higher time for detection of replica.

Figure 5 shows the comparison of average number of packets sent/received by a node per epoch versus network size. It is observed that average number of packets sent/received per epoch of the proposed scheme is higher than EDD and lower than MTLSD. This is because the only communication in the proposed scheme involves the

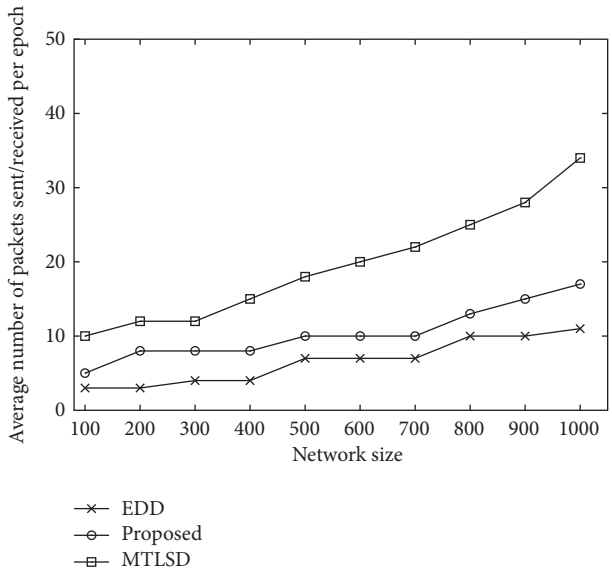

Figure 5: Comparison of average number of packets sent/received per epoch versus network size.

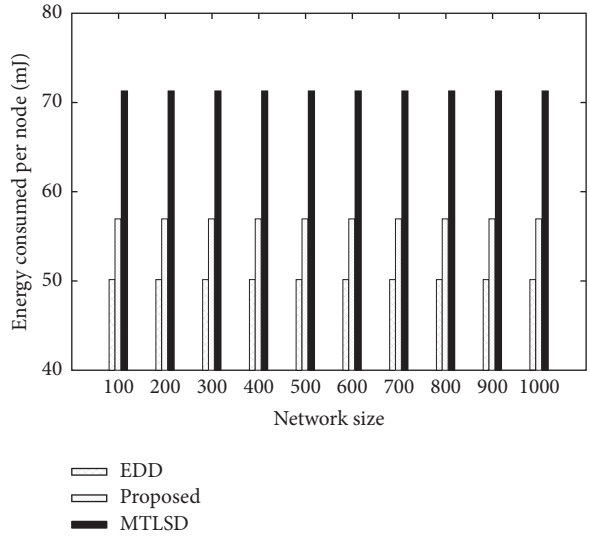

Figure 6: Comparison of energy consumed per node versus network size.

broadcasting of time-distance pair in the neighborhood. This value is quite less than the overhead of MTLSD, where all time-location claims in common are shared among the trackers. EDD has lower number of packets sent/received per node because it uses only hello broadcast message.

The energy consumed per node is compared in Figure 6. Energy consumed by the proposed scheme is higher than EDD and lower than MTLSD. This is because the energy consumption in a node mostly depends on the transmission and reception of messages. Since the communication complexity of the proposed scheme is higher than EDD and lower than MTLSD, the energy consumption per node of the proposed scheme lies between EDD and MTLSD. Finally, the plot for false positive versus network size is shown in Figure 7. The schemes considered for comparison have marginally higher

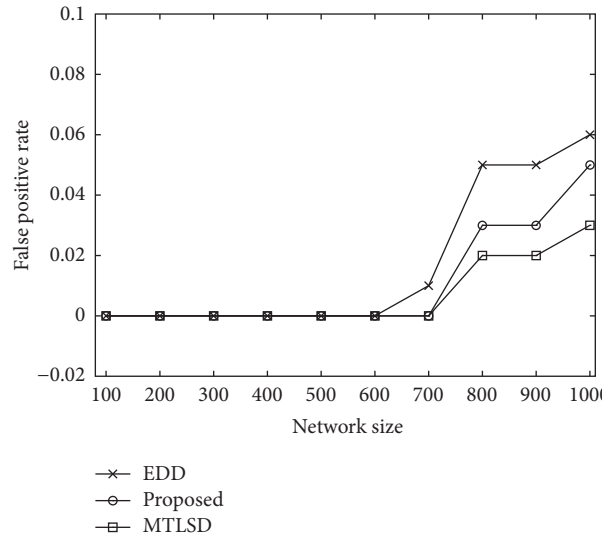

Figure 7: Comparison of false positive rate.

false positive for network size more than 700. The false positive rate is higher in EDD compared to others since it relies on number of meetings to detect replica.

7. Conclusion

In this paper, we proposed a distributed replica detection scheme for MWSNs based on sliding window approach. The scheme uses the time-distance pair to compute the degree of violation, $\deg V$. Each node acts as an observer for a number of nodes in the network. The observer nodes maintain a sliding window of recent time-distance pair of these nodes. Every mark of deviation of a replica contributes to a higher value of $\deg V$. When the degree of violation of a node is higher than η, it is detected as replica. The simulation results show that the proposed scheme has detection probability nearly equal to *one* compared to EDD and MTLSD schemes.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] M. Carlos-Mancilla, E. López-Mellado, and M. Siller, "Wireless sensor networks formation: approaches and techniques," *Journal of Sensors*, vol. 2016, Article ID 2081902, 18 pages, 2016.

[2] S. Tanwar, N. Kumar, and J. J. P. C. Rodrigues, "A systematic review on heterogeneous routing protocols for wireless sensor network," *Journal of Network and Computer Applications*, vol. 53, pp. 39–56, 2015.

[3] A. Hadjidj, M. Souil, A. Bouabdallah, Y. Challal, and H. Owen, "Wireless sensor networks for rehabilitation applications: challenges and opportunities," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 1–15, 2013.

[4] K. Sohraby, D. Minoli, and T. Znati, *Wireless Sensor Networks Technology, Protocols, and Applications*, John Wiley & Sons, New York, NY, USA, 2007.

[5] J. Rezazadeh, M. Moradi, and S. A. Ismail, "Mobile wireless sensor networks overview," *International Journal of Computer Communications and Networks*, vol. 2, no. 1, pp. 17–22, 2012.

[6] I. Amundson and X. D. Koutsoukos, "A survey on localization for mobile wireless sensor networks," in *Mobile Entity Localization and Tracking in GPS-less Environnments: Second International Workshop, MELT 2009, Orlando, FL, USA, September 30, 2009. Proceedings*, vol. 5801 of *Lecture Notes in Computer Science*, pp. 235–254, Springer, Berlin, Germany, 2009.

[7] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: attack analysis and countermeasures," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 867–880, 2012.

[8] C. Zhu, L. Shu, T. Hara, L. Wang, S. Nishio, and L. T. Yang, "A survey on communication and data management issues in mobile sensor networks," *Wireless Communications and Mobile Computing*, vol. 12, no. 16, pp. 1–18, 2011.

[9] S. Md Zin, N. Badrul Anuar, M. Laiha Mat Kiah, and A.-S. Khan Pathan, "Routing protocol design for secure WSN: review and open research issues," *Journal of Network and Computer Applications*, vol. 41, no. 1, pp. 517–530, 2014.

[10] H. Modares, R. Salleh, and A. H. Moravejosharieh, "Overview of security issues in wireless sensor networks," in *Proceedings of the 3rd International Conference on Computational Intelligence, Modelling and Simulation (CIMSiM '11)*, pp. 308–311, September 2011.

[11] D.-J. Huang and W.-C. Teng, "A defense against clock skew replication attacks in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 39, no. 1, pp. 26–37, 2014.

[12] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, "Detecting node replication attacks in wireless sensor networks: a survey," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 1022–1034, 2012.

[13] J.-W. Ho, M. Wright, and S. K. Das, "Fast detection of mobile replica node attacks in wireless sensor networks using sequential hypothesis testing," *IEEE Transactions on Mobile Computing*, vol. 10, no. 6, pp. 767–782, 2011.

[14] X. Deng, Y. Xiong, and D. Chen, "Mobility-assisted detection of the replication attacks in mobile wireless sensor networks," in *Proceedings of the 6th Annual IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '10)*, pp. 225–232, October 2010.

[15] H. R. Shaukat, F. Hashim, A. Sali, and M. F. Abdul Rasid, "Node replication attacks in mobile wireless sensor network: a survey," *International Journal of Distributed Sensor Networks*, vol. 10, no. 12, Article ID 402541, pp. 1–15, 2014.

[16] X.-M. Deng and Y. Xiong, "A new protocol for the detection of node replication attacks in mobile wireless sensor networks," *Journal of Computer Science and Technology*, vol. 26, no. 4, pp. 732–743, 2011.

[17] L. S. Sindhuja and G. Padmavathi, "Replica node detection using enhanced single hop detection with clonal selection algorithm in mobile wireless sensor networks," *Journal of Computer Networks and Communications*, vol. 2016, Article ID 1620343, 13 pages, 2016.

[18] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, "Mobile sensor network resilient against node replication attacks," in *Proceedings of the 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '08)*, pp. 597–599, San Francisco, Calif, USA, June 2008.

[19] C.-M. Yu, Y.-T. Tsou, C.-S. Lu, and S.-Y. Kuo, "Localized algorithms for detection of node replication attacks in mobile sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 5, pp. 754–768, 2013.

[20] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing* , vol. 353 of *The Kluwer International Series in Engineering and Computer Science*, chapter 5, pp. 153–181, Springer, Berlin, Germany, 1996.

[21] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology: Proceedings of CRYPTO 84*, vol. 196 of *Lecture Notes in Computer Science*, pp. 47–53, Springer, Berlin, Germany, 1985.

[22] F. Hess, "Efficient identity based signature schemes based on pairings," in *Selected Areas in Cryptography*, vol. 2595, pp. 310–324, Springer, Berlin, Germany, 2003.

[23] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 49–63, Oakland, Calif, USA, May 2005.

[24] A. Boulis, *Castalia 3.2, User's Manual*, National ICT Australia, 2011.

[25] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in *Proceedings of the 1st International ICST Conference on Simulation Tools and Techniques for Communications, Networks and Systems (SIMUTools '08)*, March 2008.