International Journal of Engineering Trends and Technology
ISSN: 2231-5381/https://doi.org/10.14445/22315381/IJETT-V70I5P237

Volume 70 Issue 5, 339-345, May 2022
© 2022 Seventh Sense Research Group®

Original Article

Replica Node Detection using Metaheuristic Algorithms in Wireless Sensor Networks

R. Bhaskaran[1], K. Ramamoorthy[2], C. Fancy[3], T. Jayasankar[4]

[1]Department of Information Technology, PSNA College of Engineering and Technology, Tamilnadu, India.
[2,4] Department of Electronics and Communication Engineering, PSNA College of Engineering and Technology, Tamilnadu, India
[3]Department of Networking and Communications, SRM Institute of Science and Technology, Tamilnadu, India.
[4] Department of Electronics and Communication Engineering, University, College of Engineering, BIT Campus, Tiruchirappalli, Tamilnadu, India.

[1]baskarpsna@gmail.com

Received: 16 March 2022 Revised: 09 May 2022 Accepted: 23 May 2022 Published: 31 May 2022

Abstract *- Clustering is one of the essential techniques to prolong the network life span in wireless sensor networks (WSNs). It comprises the clustering of mote into clusters and selecting cluster heads (CHs) for all the clusters. The main challenge in WSNs is to choose the proper CH. However, separate clusters are usually chosen; overlaying clusters are significant for the device to discover its importance in a certain process of device localization time-synchronization and inter-cluster routing. Detection of the replicate node is a significant task in overlaying clusters. This article seeks to detect replicate nodes in overlaying clusters depending on two techniques, adaptive weighted clustering (AWC) algorithm and hybrid bat algorithm with differential equation (BA-DE). The first method utilizes RFID for distinctive identification of the device, and the secondary process identifies to replicate through finding the location through Triangulation and RSSI (received signal strength) technique. These techniques are executed, and effectiveness is contrasted with non-clustered and multicast methods: Line selected multicast, Randomized multicast, K-coverage WSN, and FTVBT. The hybrid bat algorithm with differential equation (BA-DE) shows lesser communication overhead and an improved rate of detection, lesser storage cost, energy consumption, packet loss, and delay under diverse aspects because of its deterministic method.*

Keywords *- Clustering, Routing, Adaptive weighted clustering, Multicast, Differential equation.*

1. Introduction

The WSN is considered the group of dispersed sensors utilized to monitor and record the physical condition of the environment and organize the collected information in a centralized place or location for further use. The WSN have utilized in numerous fields, including animal tracking, environment, and surrounding monitoring, healthcare, security purpose, temperature, pollution level, etc. Simon Carbajo R (2017) et al. the peer-to-peer system are sometimes utilized for the same kind of operation or programs. Ez-zazi I et al. (2017) in the case of cluster system where the communication of the nodes takes place with the clusters or with the head of the clusters. Krishnan Muthumayil et al. (2021) the selection of cluster head in the cluster system is done through an election algorithm where the nodes are allowed to become the head of the cluster to avoid the one person controlling the system. The concluding process is done through an efficient system like a laptop. The openness in the system may provide a chance for attackers to attack the system or network. The need for cost in utilizing unnecessary nodes in the system, so the attack measures are not added to the single node model. The attacks in the system are categorized as Application Dependent and Independent attacks. The replication attack in the system may be termed an application-independent attack in Wireless Sensor Network. Parno B et al. (2005) in the replication attack where more than one node can be included or not included in the network, the nodes added to the system will be given with id's similar to that of the other nodes in the network. The replication attack is otherwise termed a Clone attack. Alsaedi N et al. (2017) the Sybil attack is the same as that of the replication attack in the network. Ramesh K et al. (2011) in the case of Dosl attack where the nodes get multi-ids and then it tries to launch the attack to the network system. The replication attack is detected using detection IDs. The behavior of the nodes is monitored using the node ID in the Wireless Video Sensor Network to know the misbehavior of the nodes and identify them.

2. Related Works

Mathur S et al. (2010) the Replication attack into the Wireless Sensor Network was first identified by Parrno et al., in his method where random multicast or line selected multicast is proceeded to deal with the issue of attacks in the network. In the Random Multi-cast, where the location of the nodes is chosen randomly. The node's location will be changed if two nodes hold the same location. In the case of line selected system, where the communication between the nodes takes place in sharing the location and the problem is tried to sort out by providing them a proper location. By which the nodes can participate in replication attacks. Mathur S et al.(2010), in the multicast system, the variants have to find the location for a longer period in the network system, which results in immense communication and computation. The replica detection system works with the concept of group category knowledge. The nodes present outside the home group are utilized to share locations and are capable of getting an efficient resource for the system Cho K et al. (2013) for the Line-selected multicast system. Conti et al. proposed a framework known as RED which is utilized to improve the performance of replica detection, storage capacity, and computing process.

When comparing the present system with Parrano et al., there was no better improvement in the aspects of communication. The system's protocol requires communication to multiply with the number of runs through the entire lifetime of the network. But the present scheme has more communication resources than the RED by knowing the location where the new nodes are correctly placed. Cho K et al. (2013) proposed a new scheme with an improved system known as X-RED with the same quality as RED. The major part of the design f X-RED is as same as the RED, but the witness is picked utilizing the random hash function. The present random witness selection tries to distribute eventually to all the system nodes, which saves the system from failure through a single point. The examination of the system is still not improved in the new system like other networking systems. Mathur S et al. (2010) proposed a framework for a replica detection scheme on the cell topology where the replica in this system are detected through the multicast location method, which claims to single or multiple cells. It enhances the accuracy of detection schemes proposed in Parrano et al. The network's communication resource has no improvement compared with the proposed method Cho K et al. (2013).

Ho J W et al. (2009) proposed a local replica detection system for sensors based on local or regional deployment. If the subset's intersection remains empty, then, in that case, the replicas are included in the empty subsets. There is a specific replica method where the adversary can pass the detection. Li Z et al. (2009) proposed a framework for replica detection based on group deployment where the local claim idea is adapted.

In this method, the sensor nodes present inside the home zone can transmit the message without validation; in the case of sensor nodes outside the zone are not allowed to pass the message without proper authentication. This method overcomes many disadvantages of the previous method like communication with the nodes, computing, and overheads issue because only a part of the nodes is needed for circulating and sending the location is required.

Suganthi K et al. (2015) proposed a framework using a detection algorithm to represent the problem of replication attacks in the WSN with a protocol cluster called the NI-LEACH. This protocol acts according to the performance requirement by preferring the proper encoder function. This protocol needs witness nodes for taking big computation and energy-efficient tasks. The sensor nodes pretending to witness nodes will lose energy quickly. Jobin J et al. (2004) proposed a framework for node replica detection utilizing QBM and SLSM. These two can detect the replicas, but this needs a repeat claim check by which the communication in this method will be more. The Sybil attack is the extension of the node replication attack. Arun Prakash R et al. 2018 proposed a framework capable of resisting Warmhole attack using a coordinator based that exploits the reputation ideas.

3. Proposed Methodology

The replicated nodes may present in a cluster or stay common among 2 clusters as boundary nodes. The inter and intra replication of the cluster detection process takes place to identify replica nodes from real nodes. The detection of replica nodes in the cluster-based WSN is a difficult process. This paper proposes a new localization-based node replication detection technique in cluster-based WSN using a metaheuristic algorithm and Bloom filter. Initially, the adaptive weighted clustering (AWC) algorithm is employed to organize the network into a set of clusters, and a cluster head (CH) is elected in each cluster. Then, the proposed method uses a hybridization of the bat algorithm with differential evolution (DE) to achieve accurate node localization in WSN. Next, the Bloom filter is applied to efficiently store the location details of the nodes in the network.

Finally, the node that varies from the initial node location during deployment is considered a replica node and is further eliminated from the network. The fundamental concept behind the proposed method is that it is practical to consider a node as a replica once its present location is farther from its actual location. However, the accurate location of the nodes is hard to determine due to the requirement of expensive global positional systems (GPS). Therefore, we design a hybrid BA-DE algorithm to achieve node localization. Besides, BF is used as a space-efficient probabilistic data structure, which depends upon the hashing techniques to generate the cluster member list. It is utilized in the proposed work due to its efficiency in space and simple query system. The CH has the responsibility of preparing the list, which forwards it to other cluster heads and its cluster members. Its respective cluster head will identify the replica nodes inside a cluster (intra-cluster), and the remaining CHs do the replica node between the clusters (inter-cluster) in the network. The respective cluster heads will do the intra-clustering replica node detection, and other cluster heads will execute the inter-cluster replica node in the network. Once the present location of the node significantly deviates from the actual location of the nodes, it is considered the replica node and is removed from the network. The proposed method will be implemented using the AODV protocol, and a detailed comparative analysis is made with the existing methods to ensure the effective performance of the proposed model. The proposed method effectively has a high replica detection rate, lower communication cost, storage cost, energy consumption, packet loss, and delay under diverse aspects.

4. Bloom filter

The bloom filter uses a probabilistic data structure that uses hashing to form a cluster member list. In this present study, bloom filters have been utilized because of their efficiency in space and simple query techniques for the cluster to be in memberships. The CH is responsible for preparing the membership list of the cluster.

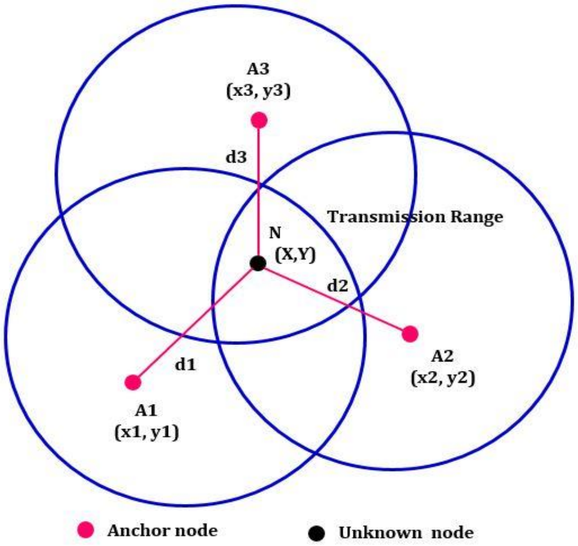

Fig. 1 Requirements of Anchor and Unknown location of nodes.

CH prepared the bloom filter list, which is forwarded to other CH. The CH would identify the nodes with more than one common cluster from this list. The cluster member is denoted as CM. The CM from cm1, cm2……….cmn belongs to CH. The cluster head calculated the value of hash for all CM. In the bloom filter, n bit is regarded as the output. By including CMi in the bloom filter, the value of the hash of cluster members CMs, with H-Hash [h1, h2 …hn] for CMi is obtained. The corresponding bit of the bloom filter will be valued as one. The bits of other bloom filters will be valued as zero. To know if cluster members are present in the bloom filter, compute the value of H to CM, and then the position for the bit is checked in the Bloom filter. If all the bits are one, the cluster member was present in the bloom filter. Algorithm 1 was based on insertion, and algorithm 2 was based on steps involved in the query of the bloom filter. About the concept of insertion algorithm, no CM will not be leftover in BF. It was considered the reason for zero false negatives in BF. In the bloom filter possibility for non-CM to be marked as CM. shows that there is the possibility of a fake positive. The probability of a false positive in a BF is

$$p = \left(1 - \left(1 - {}^{1}/_{m}\right)^{kn}\right)^{k} \tag{1}$$

m refers to the number of bits in BF, k- number of time for the hash function to be executed in the process of generating the value of H in the cluster member id, n- total nodes in the clustering system, equation 1 will be described as

$$p = \left(1 - e^{-kn/m}\right)^{k} \tag{2}$$

K-hash function number can be described as

$$k = \frac{m}{n} ln2 \tag{3}$$

Substituting k in (2),

$$p = \left(1 - e^{-({}^{m}/_{n} ln2)\, n/m}\right)^{\frac{m}{n} ln2} \tag{4}$$

Eq. (4) is further simplified as

$$lnp = -\frac{m}{n}(ln2)^2 \tag{5}$$

From (5), m can be obtained as

$$m = \left|\frac{nlnp}{(ln2)^2}\right| \tag{6}$$

4.1. Localization

The BA-DE method utilizes localization for finding the node location in clusters. The difference in distance between the unknown and the known node is measured using triangulation which combines with RSSI. The distance obtained can be used for determining the position of the unknown node. 3 anchor nodes are needed to find the unknown node location. The distance of Euclidean of the unknown node, the three anchor nodes in the triangulation method, is the reason behind providing with perfect location of the nodes in the system. The distance of the nodes is computed using RSSI. From the computed distance, the location of the anchor node, an unknown node, can be identified. Algorithm 3 is based on location computing utilizing triangulation and Received Signal Strength Indicator.

5. Adversary system and the hypothesis

The adversary model aims to clone or replicate the current nodules in the network. These cloned or replicated devices can act like real devices and might attempt to attack additional devices. A multi-hop clustering-based wireless sensor network is considered in the forecasted system in which all devices are deemed to be in the same way. The devices are supposed to have a distinctive ID. All the devices are location-unaware apart from some anchor devices. The system does not need a system or base station to manage the events of subgroups of devices due to its distributed and decentralized nature. The devices are organized on their own to reach collective decisions and need collaboration between them. The scheme presumes that the mote is static, and they communicate at the transmission range and similar power level. The suggested method also presumes a fundamental security system in the suggested networking model. The Current encryption algorithms are secure for decrypting and encrypting data. Correspondingly, current techniques for exchanging keys and construction may be utilized. The forecasted technique also entails the number of real devices to be higher than 55% of the overall devices in the network. These statements are affected because these options do not influence the outcome of the forecasted method. The forecasted technique also presumes that there are the current routing methods.

6. Randomized communication complexity

TheThe bloom filter message swap takes place among the CH. Consequently, the interaction difficulty of the system varies primarily on the amount of CH. Assuming

c= the amount of CH,

cm= the amount of cluster members,

n= the number of devices in the network.

The O(c2)- communication occurs randomly when the cluster head exchanges 2(c-1)- messages.

A device transmits its neighbour id in N2NB and its geographical position claim to the nearby devices. The nearby devices transmit the detailed information of the received messages to its nearby device.

The device can identify the replica when it notices the contradictory claim. The demographic location of the DM and N2NB are transferred. The witness devices are responsible for recognising the replica. Witness devices perform the monitoring procedure. Because both the techniques use the transmitting method for replica detection, O(n2) – communication complexity. In LSM, O (n √n)- communication complexity. A device pass on a collected geographical position claim to a chosen device in LSM. The device choice depends on rumour routing. As the geographical position claim is sent on a specific path, contradictory allegations can be found at the interconnection goals of the path. In DM, LSM, and N2NB, the location claims and received device ids have to be dispatched by the devices. The bloom filter is utilized in forecasted techniques. The information that includes the entire device cluster-id is dispatched in the form of a single bit list of CH. The randomized communication complexity of the planned methods is less significant in comparison to the LSM, DM, and N2NB when

$$n^2(|id|) > n\sqrt{n}(|id|) > C^2(m) \tag{7}$$

m can be decided by (8) as

$$m = -\frac{nlnp}{(ln2)^2} \tag{8}$$

When c ≤ n2|id| (ln 2) 2 − ln p, the intended techniques are highly effective than DM and N2NB.

It is stated that c is not more than n; therefore, it may be determined that once c≤ √n|id| (ln 2) 2 − ln p, the projected methods are effective compared to Line Selected Multicast. Utilizing these factors, the cost of communication in the forecasted technique for 1500 devices with 100 cluster members and 15 clusters is 20 BF of 1250 length of the bits. The communication cost is reduced because the bloom filter has reduced the data regarding the whole CM within a single array. Additional interaction may be needed for replica verification which is insignificant.

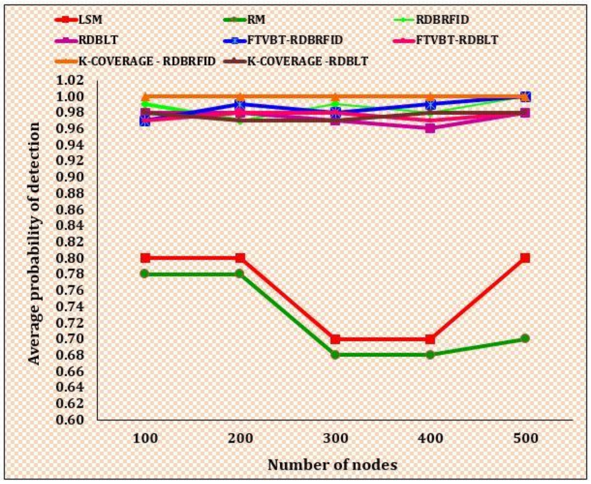

Fig. 2 Average possibility of detection Vs. number of devices for existing and forecasted method

7. Modelling Results

Fig.4 and Fig. 5 display the detection possibility of the forecasted technique adaptive weighted clustering (AWC) algorithm and BA-DE for a diverse amount of replica nodes. The replica nodes may be the CH or normal mote. The h – value differs between one and two, and the findings are achieved. All the duplicated devices have been positioned at random in the network at the start of the models. The method BA-DE for differing h provides an improved detection possibility of more than ninety-six percent. The possibility rate for detecting the intended techniques declines alongside a rise in the number of replicate nodes. This is due to the confirmation of BF loss in the replicate nodes being selected during the authentication procedure. It stated that when the h-value rises, the size of the cluster also rises, and thus amount of CH declines. Rising the number of replica nodes, the median rate of replica detection is discovered, and the rate of detection of the forecasted technique adaptive weighted clustering (AWC) algorithm and BA-DE are shown in Fig. 6. When the amount of CH declines, the communication overhead also decreases. The sum of devices is a hundred; hop count is 2 & 1, and replicate nodes range between 6 and 35.

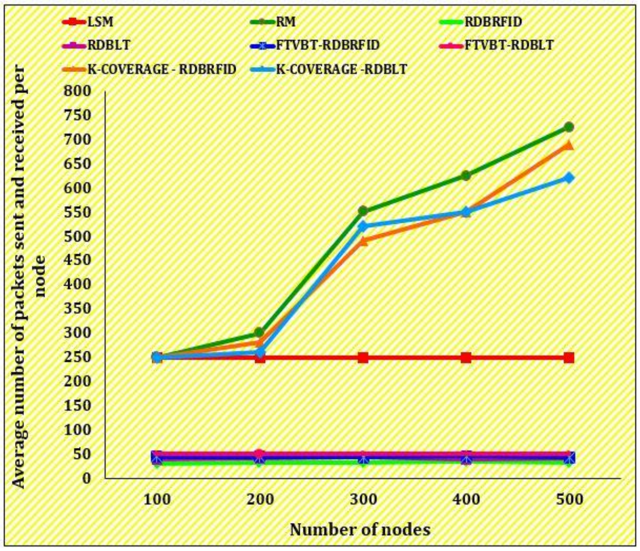

Fig.3 Communication overhead for forecasted and existing algorithm

The median possibility of the detection rate is noticed to be ninety-eight percent for the adaptive weighted clustering (AWC) algorithm and ninety-seven percent for BA-DE.

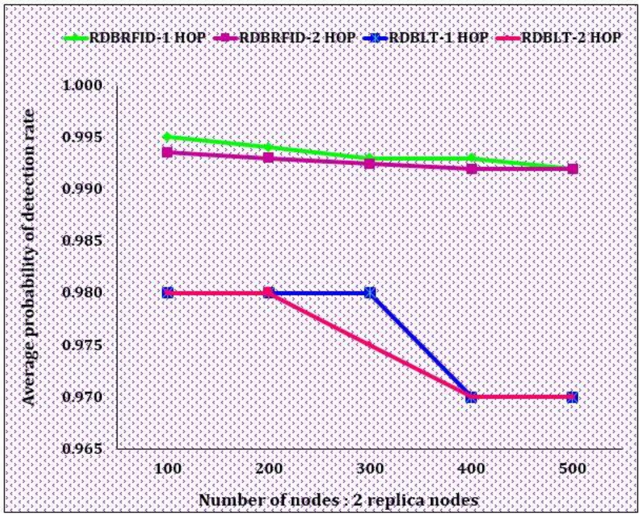

Fig. 4 Cloned device detection probability for 10 cloned devices for forecasted algorithm

Fig. 7 shows the probability gain for evaluating the two forecasted techniques adaptive weighted clustering (AWC) algorithm and BA-DE. The outcomes were obtained for differing hop count 2 & 1. The probability gain of the adaptive weighted clustering (AWC) algorithm over BA-DE differs between 1.02% and 1.03%. It is realized that this variation is due to the determinative nature of the forecasted technique adaptive weighted clustering (AWC) algorithm in comparison to the BA-DE method.

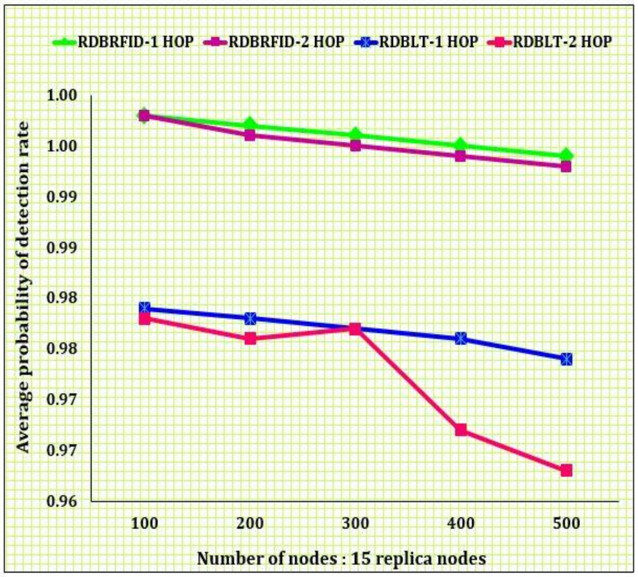

Fig. 5 Cloned device detection possibility for 15 duplicated devices for forecasted algorithm

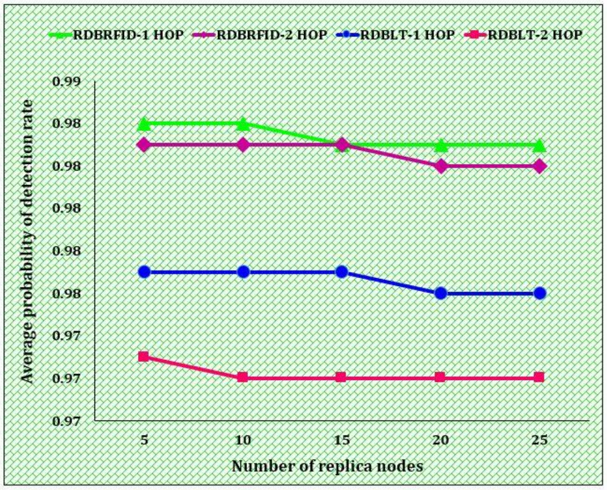

Fig. 6 Average possibility of the rate of detection for a different amount of replica node for forecasted algorithm

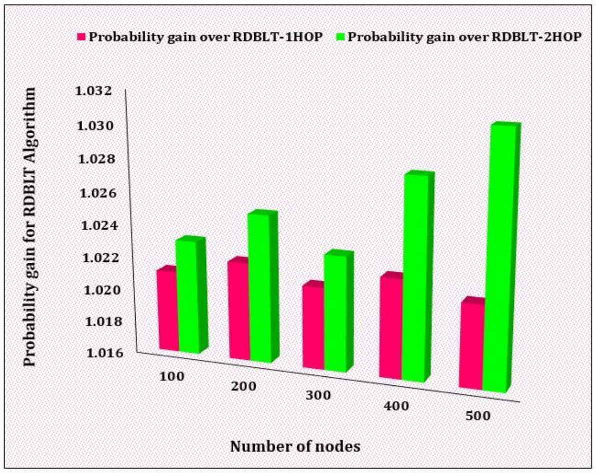

Fig.7 Probability gain of forecasted algorithm

5. Conclusion

In overlapping clusters, the most important challenging task is replica node detection because the cluster members are distributed among the clusters. The techniques of adaptive weighted clustering (AWC) algorithm and BA-DE address the problem by utilizing Localization and RFID. The techniques are compared to LSM and RM systems, and their effectiveness is examined. The techniques are further detected in non-cluster situations K-coverage, and FTVBT Wireless Sensor Network for analyzing the efficiency and the findings are discovered. It is stated that the forecasted techniques adaptive weighted clustering (AWC) algorithm and BA-DE provide minimum communication overhead in comparison to the existing methodologies. The forecasted method will be implemented using the AODV protocol, and a detailed comparative analysis is made with the current methods to ensure the effective efficiency of the forecasted model. The forecasted method is effective with a high replica rate of detection, lower communication cost, storage cost, energy consumption, packet loss, and delay under diverse aspects.

Conflicts of Interest

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

Funding Statement

The authors received no specific funding for this study.

References

[1] R. S. Carbajo, and C. Mc Goldrick, Decentralized Peer-to-Peer Data Dissemination in Wireless Sensor Networks, Pervasive Mobile Comput. 40(1) (2017) 242– 66.

[2] I. Ez-zazi, M. Arioua, A. El Oualkadi, and P. Lorenz, On the Performance of Adaptive Coding Schemes for Energy-Efficient and Reliable Clustered Wireless Sensor Networks, Ad Hoc Network. 64(1) (2017) 99–111.

[3] Krishnan Muthumayil, Thangaiyan Jayasankar, Nagappan Krishnaraj, Mohamed Sikkandar, Prakash Nattanmai Balasubramanian and Chokkalingam Bharatiraja, Maximizing Throughput in Wireless Multimedia Sensor Network using Soft Computing Techniques, Intelligent Automation & Soft Computing. 27(3) (2021) 771-784. Doi:10.32604/iasc.2021.012462

[4] B. Parno, A. Perrig, and V. Gligor, Distributed Detection of Node Replication Attacks in Sensor Networks, In: IEEE International Conference on Security and Privacy. 1(1) (2005) 49–63.

[5] N. Alsaedi, F. Hashim, A. Sali, and FZ. Rokhan, Detecting Sybil Attacks in Clustered Wireless Sensor Networks Based on Energy Trust System (ETS), Comput Commun. 2017(110) (2017) 75–82.

[6] S. Ramesh, C. Yaashuwanth, K. Prathibanandhi, Adam Raja Basha and T. Jayasankar, An Optimized Deep Neural Network-Based Dos Attack Detection in Wireless Video Sensor Network, Journal of Ambient Intelligence and Humanized Computing (2021). https://doi.org/10.1007/s12652-020-02763-9.

[7] S. Mathur, A. Reznik, C. Ye, R. Mukherjee, A. Rahman, and Y. Shah, Exploiting the Physical Layer for Enhanced Security, IEEE J Wirel Commun. 17 (2010) 63–70.

[8] K. Cho, M. Jo, T. Kwon, H. H. Chen, and DH. Lee, Classification and Experimental Analysis for Clone Detection Approach in Wireless Sensor Networks, IEEE Syst J. 7(1) (2013) 26–35.

[9] Z. Jinchao, Research on the Key Pre-Distribution Scheme of Wireless Sensor Networks, In: International Conference on Intelligent Computation Technology and Automation. 1(1) (2012) 287–90.

[10] J. W. Ho, D. Liu, M. Wright, and S. K. Das, Distributed Detection of Replica Node Attacks with Group Deployment Knowledge in Wireless Sensor Networks, J Ad Hoc Network. 7(8) (2009) 1476–88.

[11] Z. Li, and G. Gong, Randomly Directed Exploration: An Efficient Node Clone Detection Protocol in Wireless Sensor Networks, IEEE Int Conf Mobile Ad-hoc Sens Syst. 12(1) (2009) 1030–5.

[12] B. Zhu, VGK. Addada, S. Setia, S. Jajodia, and S. Roy, Efficient Distributed Detection of Node Replication Attacks in Sensor Networks. Comput Secur Appl. 2007 (2007) 257–66.

[13] M. Zhang, V. Khanapure, S. Chen, and X. Xiao, Memory Efficient Protocols for Detecting Node Replication Attacks in Wireless Sensor Networks. In proc. Int Conf Network Proto. (2009) 284–93.

[14] Z. Qin, C. Ma, L. Wang, J. Xu, and B. Lu, An Overlapping Clustering Approach for Routing in Wireless Sensor Networks, Int J Distrib Sens Network. 1 (2012) 1–13.

[15] M. Cunche, I Know Your MAC Address: Targeted Tracking of Individuals using Wi-Fi, In: International Symposium on Grey-Hat Hacking. (2013) 1–18.

[16] K. Suganthi, B. Vinayaga Sundaram, and J. Aarthi, Randomized Fault-Tolerant Virtual Backbone Tree to Improve the Lifetime of Wireless Sensor Networks. Comput Electric Eng. 48 (2015) 286–97.

[17] J. Jobin, SV. Krishnamurthy, and SK. Tripathi, A Scheme for the Assignment of Unique Addresses to Support Self-Organization in Wireless Sensor Networks. Int Conf Veh Technol. 6 (2004) 4578–4582.

[18] N. Jaiswal. An Overview of WSN and RFID Network Integration, In: International Conference on Electronics and Communication Systems. (2015) 497–502.

[19] R.ArunPrakash, W. R. Salem Jeyaseelan, T.Jayasankar, Detection, Prevention and Mitigation of Wormhole Attack in Wireless Ad HoNetwork by Coordinator, Appl. Math. Inf. Sci. 12(1) (2018) 233–237. Doi: http://dx.doi.org/10.18576/amis/120123

[20] G. Mao, and B. Fidan. Anderson BDO, Wireless Sensor Network Localization Techniques, Comput Network. 51(10) (2007) 2529–53.

[21] S. Geravand, and M. Ahmadi, Bloom Filter Applications in Network Security: A State-of-the-Art Survey, Comput Network. 57(18) (2013) 4047–4064.

[22] (2012). [Online]. Available: https://en.wikipedia.org/wiki/Bloom_filter

[23] Z. Qin, C. Ma, L. Wang, J. Xu, and B. Lu. An Overlapping Clustering Approach for Routing in Wireless Sensor Networks, Int J Distrib Sens Network. 1 (2012) 1-13.

[24] (2009). [Online]. Available: https://www.cryptopp.com/benchmarks.html.

[25] (2012). [Online]. Available: https://www.das-labor.org/wiki/AVR-Crypto-Lib/en.

[26] D.E. Knuth. The Art of Computer Programming, 3rd ed., Addison-Wesley, Newyork. (1997).

[27] (2012). [Online]. Available: http://www.isi.edu/nsnam/ns/.

[28] X. Wang, J. Wu, L. Guo, A k-coverage Algorithm in Three-Dimensional Wireless Sensor Networks, In: IEEE International Conference on Broadband Network and Multimedia Technology. (2010) 1089–93.