Elliptical Curve Diffe-Hellman Algorithm for discovering Duplication Attack in Mobile WSN

J. Shirisha
Department of Electronics and Communication Engineering, Malla Reddy Engineering College (Autonomous)
Hyderabad, Telangana, India.
shirisha.gangam401@gmail.com

R.Sabitha
Department of Computer Science and Engineering, Rajalakshmi Engineering
Chennai, Tamil Nadu, India
sabisam73@gmail.com

M. Rajkumar
School of Information Technology and Engineering, VIT University, Vellore Campus,
Vellore, Tamil Nadu, India.
mrajkumarselvee@gmail.com

B.Maruthu Kannan
Department of Computer Science and Engineering Sphoorthy Engineering College,
Nadergul, Hyderabad, Telangana, India
lampsuccess@gmail.com

Sangeetha D P
Department of Electronics and Communication Engineering, Sona College of Technology,
Salem, Tamil Nadu, India
sangitasankarslm@gmail.com

S. Renukadevi
Department of Mathematics, Bharathi Women's College (Autonomous)
Chennai, Tamil Nadu, India
dr.s.renukadevi@gmail.com

2022 International Conference on Computer, Power and Communications (ICCPC) | 979-8-3503-9784-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCPC55978.2022.10072042

***Abstract*—Wireless Sensor Network (WSN) is the greatest susceptible of all the wireless sensor nodes. In the WSN, several widespread attacks were launched in the rival world. The most problematic are complete attack identification and avoidance of node duplication. The period it takes to recognize and separate a duplicated sensor node is typically higher than other attack recognition methods owing to the related identity and features copied through the attacker. Elliptical Curve Diffe-Hellman Algorithm is employed for discovering duplication attack (ECDD) in Mobile WSN. This approach aims to distinguish duplicated sensor nodes in the mobile WSN. In this approach, the public and private keys are used for verification. The ECDD method interacts with the secret key to distinguish the duplicate sensor node and separate it from routing, raising the network function. The simulation examination demonstrates a lesser false negative ratio and increases duplicate attack detection in the network.**

Keywords*—Duplication Attack Detection, Wireless Sensor Network, Elliptical Curve Diffe-Hellman, Sensor Mobility, and Key Verification.

I. INTRODUCTION

Mobile WSN is a self-organized multi-hop structure included several mobile nodes. Mobile WSN does not have any pre-set infra-structure and comprises the numerous sensor nodes that moving energetically not comprising any boundary restrictions. Benefits are quick to connect, provide fault tolerance, connectivity, and sensor node movement. Though, the mobile WSN tasks are the active topology, open medium, bandwidth reserved; link capability, energy-restrained function, and also insufficient physical protection. Lacking security, the attacker simply attacks the WSN during data communication [1].

WSNs have uncovered an extraordinary level of expansion in the modern world. WSNs have become the central processing unit of an increasing number of automation and control systems. The advancement in perception has not only favoured the expansion of charity and peace over the globe, but it has also generated desire among the adversaries; as a result, the WSN is more vulnerable to assaults in the likely and risky functions. The use of a wireless media contributed further to the vulnerability that serves as the root cause of the occurrence of active and passive assaults [2]. The replication assault, which was shown to be a unique security risk, is one of the most malicious attacks that has ever been carried out. Due to the fact that this kind of attack compares the attributes of the duplicated node with those of the actual node, it poses a significant risk to the discrimination process. Any inner node may be seized by unlicensed individuals, and its identified attributes can be simulated into a new node that can later be tossed into an actively operating WSN to make it function as a separate genuine node [3]. Figure 1 explains the Mobile WSN with duplication attacker.

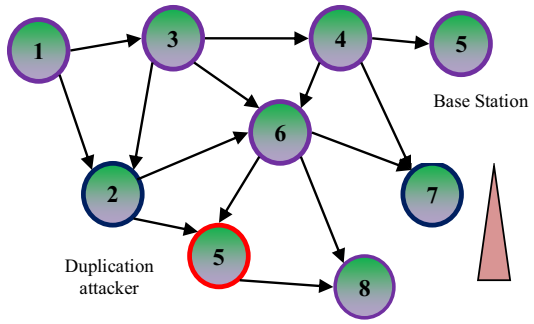

Fig.1. Example diagram of Mobile WSN

There are many different kinds of security breaches that may occur in today's world, including wormhole breaches, duplication assaults, denial of service breaches, cyber security breaches, routing breaches, Sybil breaches, jamming breaches, physical breaches, and black hole breaches, amongst others. In MWSN, a dangerous kind of assault is the duplicate node attack. An advisory may seize control of the mobile node in order to get the data that is kept in it, and it is then able to produce many copies of the mobile node that it has taken control of [4]. As a result, the success of a duplicating attack is ultimately determined by how quickly a destructive action may be started in the network. An advice overcomes the challenges presented by the unattended nature of a compromised node and retrieves all of the data stored in its memory, including the node's key, identity, and other information relevant to connecting with other nodes. In addition, an advisory may replicate the mobile node that was seized and then reintroduce it to the network at the location that it was intended for. After that, the advisory may utilize the compromised mobile node to monitor and manipulate the various functionalities using it. Because of this, the failure to notice the duplicate node in a timely manner might result in significant damage [5].

One of the most important forms of malicious node assault is the replication attack. The attacker must first take control of a valid node and steal all of the secret information before launching a duplicate assault. Following that, it is able to spread duplicate nodes over the network in [8] by asserting the same identity as the node that it has captured. Colliding identities and being in distinct places are the cornerstones of the duplicate detection process [6].

To provide further clarification, duplicate nodes and captured nodes are physically located in distinct parts of the network, despite the fact that both types of nodes claim to have the same identity. This article will go over four methods for detecting a duplication assault. These methods are known as deterministic multicasting, node-to-network broadcasting, line-selected multicasting (LSM), and randomized multicasting. Node-To-Network Broadcasting is a preliminary method for detecting collisions between identities. It does this by flooding the network with information about locations [7]. In addition, the information is broadcast through deterministic multicast to a number of specified witness nodes. Alternately, a random selection process is used by randomized multicast to choose witness nodes. LSM is responsible for designating witness nodes at the back by following route lines. As a direct consequence of this, the duplication assault may, at the very best, be identified at the intersections of witness route lines. It chose witnesses by wandering about in a random pattern rather than travelling along predetermined paths. As a future stage, two routing algorithms are designed with the goals of lowering the cost of memory and increasing the lifespan of the network. [8].

II. Related Works

MWSNs, which have the benefit of movable nodes that can regulate their own mobility, have been the primary focus of the majority of research in recent years. In addition, it has been shown that mobility lessens the challenges that arise with respect to the maximum coverage area and connection. Nevertheless, the assessment of the positions of mobile nodes is the most crucial job in MWSNs. In recent years, several applications for execution mobility have begun to play a significant part in a particular category of wireless sensor networks (WSNs) known as MWSNs.

A malicious-node identification approach avoids fault information injection attacks using correlation theory. Initially, an abnormality among same sensor information is noticed through time correlation. Next, the malicious nodes are recognized using the spatial correlation. Finally, the event correlation is utilized to recognize malicious nodes [9]. Markov model is used for evaluating the sensor node reliability approach that observing and unimodal operation [10]. This approach concentrate on whether a single otherwise multiple sinks are engaged, nodes are static and mobile [11]. Elliptic curve cryptography (ECC) is lengthily utilized in several multifactor authentication approaches. The threat model deliberates several kinds of attacks comprising Man In the Middle (MIM), weak authentication, and denial of service. Countermeasures to decrease otherwise evade this attacks are advised. Intrusion Detection System (IDS) is used for prevent the MIM attack. The IDS occasionally catechise nodes one hop away [12]. Elliptic Curve Diffie Hellman key interchange is investigated applying PyCryptodome package and the Integrated Encryption method of Elliptic Curve. Authentication also statistics encryption method is for node-to-node transmission. Elliptic Curve Digital Signature method is to offer a suitable mechanism for evaluating the time of key generation, size of the packet and hello message count. This approach assists in obtaining the complete network in a better and effective method. This approach minimizes the cost risk and threats of security on authentication [13].

ECC is an efficient key owing to it is a smaller size key. Hence, it minimizes the unwanted energy utilization. ECC is a faster transmission, rise for serious operation, thus enormous injuries are triggered through intrusion attacks [14]. Adaptive Multi-Token Approach establishes secure authentication which applies ECDH method with Dynamic Token Ring approach. This approach deals with intra, and inter-flow disputation issues the help of a Dynamic Token Ring. It offers solution for inter-flow/intra-flow dispute issues also hidden and exposed terminal issues [15]. This approach provides a position established rewarding method here the node can gather position-built tokens from token distributers, and recycle the gathered tokens for helpful rewards. This approach offers smaller overhead and protected data communication [16].

An energy efficient method established public key cryptography method attains instant authentication and it avoid Denial of Service attacks [17]. It extended Identity Based Encryption (EIBE) approach that makes sure authentication also confidentiality. Here, the Kerberos authentication approaches plus Identity Based Encryption to confirm authentication and privacy [18]. A glaucoma diagnosis applying Convolutional Neural Network is for detecting the spectral colour. Here, colour modules are divided as red, green, and blue. Next, the green channel is applied for the image analysis and detection [19]. The Dynamic Traffic Management is control of traffic signals for high traffic places in the network [20]. Enhanced Node Selection Technique is used for improving the multipath routing. This method responsible the optimized node which assists route detection and enhance the quality of service in the WSN. Here, selects the route by node received signal strength and remaining energy [21]. The aim of trust-based system in [22] is to classify and separating the several attacks in the network.

In general, duplicate content finders may be broken down into three categories: textually based, token-based, and structurally based code clone detection methods. The textual-based approaches are able to express snippets of code in the form of strings. In the event when the text contents of the two code fragments are comparable, then the two code fragments are regarded as duplication nodes [23]. The source code is represented as a list of token sequences, and a variety of similarity detection methods are used to the token sequences in order to find duplicates of the source code. The techniques identify instances of code duplication by parsing the syntax of the code in order to determine the semantic characteristics of the code [24].

Testing the efficacy of code duplication detectors is another application for mutation testing that may be carried out. It then employed dynamic clustering to do basic text-line comparisons of probable duplications [25], after first identifying and standardizing potential duplications. A technique for testing code duplications uses mutation insertion is discussed. In order to artificially forge various

types of code duplication pairs, which can then be tested against the target duplication detectors [26], the idea is to re-insert an artificial piece of code into a piece of source code. This will allow different types of code duplication pairs to be artificially forged. A approach for evaluating the robustness of several classic code duplication detectors that uses code obfuscation. They obfuscated the source code by applying a few code mutations in a semi-automatic manner and did not explore any techniques that would guide the code mutation. This method's objective is to perform a simple modification that is yet powerful in order to produce semantic duplications that are capable of fooling learning-based as well as more conventional forms of duplication detection [27].

III. Proposed Method

A duplicated sensor node may drop the packet otherwise changes the packet throughout data communication. Primarily, the network distributed number of sensor nodes with a Base Station (BS). The BS is a reliable that is accountable for disseminated detection. All sensor nodes have the equal transmission range. In this approach, the malicious nodes are able to capture the number of mobile sensor nodes in the network and the malicious nodes control sensor nodes denoted as duplication nodes. Adversaries reproduce replicas of captured nodes called as a duplication nodes. In this approach this uses ECDH technique for detecting the participating duplicate sensor nodes. In this approach, the key ECDH is done through the subsequent procedures. The simple Weierstrass expression is given below.

$$Y^2 = X^3 + aX + b \qquad (1)$$

Each sensor node is allocated the private key; such key is preserved in top-secret. The private key (PR_K) is assessed the expression is given below.

$$PR_K = \sum_{j=0}^{h} N_j \qquad (2)$$

Here, Nj represent the sensor node

h indicates the hop count

The sender distributes the Route Request (RREQ) message to its neighboring nodes. This RREQ message consists of sender sensor node identity, receiver node identity, and sender public key. This public key (PUK) is computed through the equation is given below.

$$PU_K = \sum_{j=0}^{h} N_j * \beta \qquad (3)$$

Here, β represents the elliptic curve

The receiver sensor obtains the sender forward the message then send R_{REP} message back to the sender. This Route Reply (R_{REP}) message comprises the receiver secret key. This secret key is evaluated through the equation is given below.

$$SE_K = \sum_{j=0}^{h} PR_K * PU_K \qquad (4)$$

All sensor nodes are certified by applying the ECDD authentication procedure. If the node success the confirmation, next the data is forwarded to the proved node. If the sensor node notices the duplicated node, next notice the details to whole nodes and isolate that node from the network.

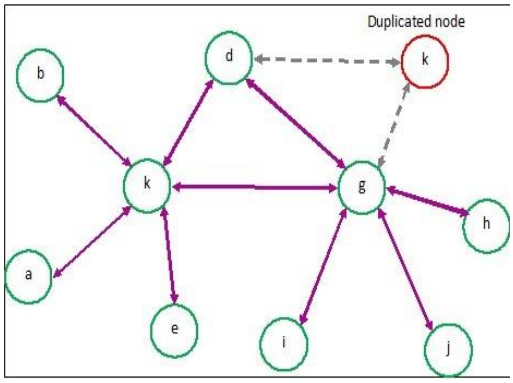

Fig. 2. ECDD Verification among Nodes.

Figure 2 illustrates the ECDD verification among nodes in the mobile WSN. From this figure, the two sensor nodes have same identity k. The sender confirms the k secret key. Here, real sensor node verifies the secret key but, the duplicated node k is not verified the secret key. Finally, the sender discovers the duplicated node. Then, the sender forwards the notification message to all nodes. All nodes are isolating the duplicated node in the mobile WSN.

IV. Simuation Analysis

The proposed ECDD approach is implemented applying Network Simulator -NS-2.34. This practices the network region of topology is 650 × 250 meter square. Here, the Mobile WSN by 30 sensor nodes is made. These sensor nodes are freedom to move one place to another place. The Constant Bit Rate (CBR) is used for the traffic model in the mobile WSN. The duplicate attack detection ratio and false negative ratio value parameters are measured the efficiency of ECDD approach. Figure 3 and Table 1 show the detection ratio of EIBE and ECDD approaches.

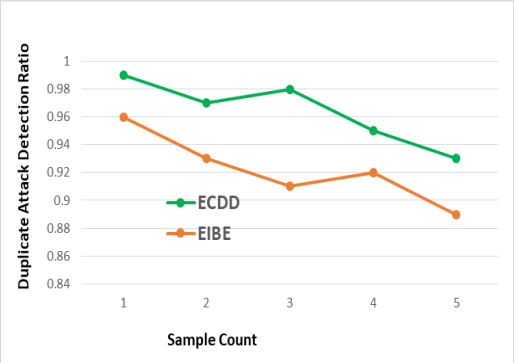

Fig. 3. Duplicate Attack Detection Ratio of EIBE and ECDD.

TABLE I. DUPLICATE ATTACK DETECTION RATIO VALUES OF EIBE AND ECDD APPROACHES

Sample Count	ECDD	EIBE
1	0.99	0.96
2	0.97	0.93
3	0.98	0.91
4	0.95	0.92
5	0.93	0.89

From Figure 3 and Table 1, the conventional method EIBE approach is very lowest detection performance compared to the ECDD approach. But ECDD approach gives the better performance in the WSN. Figure 4 and Table 2 illustrate that false negative ratio of EIBE and ECDD approaches.

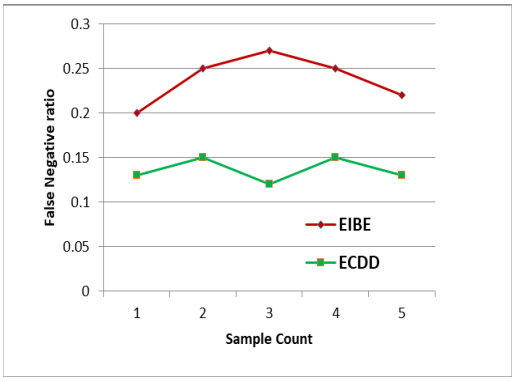

Fig. 4. False Negative Ratio of EIBE and ECDD.

TABLE II. FALSE NEGATIVE RATIO OF VALUES OF EIBE AND ECDD APPROACHES

Sample Count	ECDD	EIBE
1	0.14	02
2	0.15	0.25
3	0.12	0.27
4	0.15	0.25
5	0.12	0.21

From Figure 4 and Table 2, the conventional method EIBE approach is highest false negative ratio compared to the ECDD approach. But ECDD approach gives lesser false negative ratio as a result, raises the better function in the WSN.

V. CONCLUSION

The duplication attack was confirmed as an exclusive security threat among the most spiteful attacks. This attack is a severe threat to discriminate the comparison in the features among the duplicated and the actual node. Any interior node is taken through unlicensed persons, and the detected elements are simulated into their new node that is future thrown into an energetically acting WSN to create it work like a specific legitimate node. This approach presents Elliptical Curve Diffe-Hellman Algorithm for discovering duplication attacks in Mobile WSN. This approach aims to distinguish duplicated sensor nodes. In this approach, the public and private keys are used for verification. The ECDD method interacts with the secret key to determine the duplicate sensor node and separate it from routing, raising the network function. The simulation examination demonstrates a lesser false negative ratio and increases duplicate attack detection in the network.

REFERENCES

[1] A. K. Al-Ani, M. Anbar, A. Al-Ani, and D. R. Ibrahim, "Match-prevention technique against denial-of-service attack on address resolution and duplicate address detection processes in IPv6 link-local network," IEEE Access, vol. 8, pp. 27 122–27 138, 2020.

[2] S. U. Rehman and S. Manickam, "Denial of service attack in IPv6 duplicate address detection process," Int. J. Adv. Comput. Sci. Appl, vol. 7, pp. 232–238, 2016.

[3] H. R. Shaukat, F. Hashim, and A. Sali, "Danger theory based node replication attacks detection in mobile wireless sensor network," 2014 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE), pp. 18–23, 2014.

[4] M. Numan, F. Subhan, W.Z. Khan, S. Hakak, S. Haider, G.T. Reddy, & M. Alazab, "A systematic review on clone node detection in static wireless sensor networks," IEEE Access, vol. *8*, pp. 65450-65461.

[5] P.P. Devi, & B. Jaison, Protection on wireless sensor network from clone attack using the SDN-enabled hybrid clone node detection mechanisms. Computer Communications, vol. 152, pp. 316-322, 2020.

[6] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks," IEEE J. Sel. Areas Commun., vol. 28, no. 5, pp. 677–691, 2010.

[7] M. Dong, K. Ota, L. T. Yang, A. Liu, and M. Guo, "LSCD: A lowstorage clone detection protocol for cyber-physical systems," IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst., vol. 35, no. 5, pp. 712–723, 2016.

[8] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, "Energy and memory efficient clone detection in wireless sensor networks," IEEE Trans.Mobile Comput., vol. 15, no. 5, pp. 1130–1143, 2016.

[9] Y. Lai, L. Tong, J. Liu, Y. Wang, T. Tang, Z. Zhao, and H. Qin, "Identifying malicious nodes in wireless sensor networks based on correlation detection," Computers & Security, vol. 113, pp. 102 540–102 540, 2022.

[10] I. Kabashkin and J. Kundler, "Reliability of sensor nodes in wireless sensor networks of cyber physical systems," Procedia Computer Science, vol. 104, pp. 380–384, 2017.

[11] J. Al-Muhtadi, M. Qiang, K. Zeb, J. Chaudhry, K. Saleem, A. Derhab, Pasha, and M, "A critical analysis of mobility management related issues of wireless sensor networks in cyber physical systems," IEEE Access, vol. 6, pp. 16 363–16 376, 2018.

[12] B. Nair and C. Mala, "Analysis of ECC for application specific WSN security," 2015 IEEE International Conference on Computational Intel- ligence and Computing Research (ICCIC), pp. 1–6, 2015.

[13] M. F. Moghadam, M. Nikooghadam, M. A. B. A. Jabban, M. Alishahi, L. Mortazavi, and A. Mohajerzadeh, "An efficient authentication and key agreement scheme based on ECDH for wireless sensor network," IEEE Access, vol. 8, pp. 73 182–73 192, 2020.

[14] U. Iqbal and S. Shafi, "A provable and secure key exchange protocol based on the elliptical curve diffe-hellman for wsn," in Advances in big data and cloud computing. Springer, 2019, pp. 363–372.

[15] N. Thangarasu, "Implementation secure authentication using elliptic curve cryptography," Int. J. Innovative Res. Adv. Eng.(IJIRAE), no. 1, pp. 1–1, 2014.

[16] D. He, J. Bu, S. Zhu, S. Chan, and C. Chen, "Distributed access control with privacy support in wireless sensor networks," IEEE Transactions on wireless communications, vol. 10, no. 10, pp. 3472–3481, 2011.

[17] H. Ghasemzadeh, A. Payandeh, and M. R., "Key management system for WSNs based on hash functions and elliptic curve cryptography," 2017.

[18] K. Prabakaran and M. Prabu, "Secure And Efficient Data Contribution Using Extended Identity Based Encryption In Cloud Computing," Inter- national Journal of MC Square Scientific Research, vol. 9, no. 1, 2017.

[19] N. C. Sendhilkumar and P. Subramanian, "Dynamic Traffic Management System using Infrared and Internet of Things," International Journal of MC Square Scientific Research, vol. 13, no. 1, 2021.

[20] A. Unnikrishnan, V. Das, "Cooperative Routing For Improving The Lifetime Of Wireless Ad-Hoc Networks," International Journal of Advances in Signal and Image Sciences, vol. 8, no. 1, pp. 17–24, 2022.

[21] S. Rameshkumar, "Improving Quality of Service through enhanced node selection technique in Wireless Sensor Networks," International Journal of MC Square Scientific Research, vol. 8, no. 1, 2016.

[22] D. Rajesh, S. K. Jahana, R. Sivakalai, and J. M. Banu, "Detection And Isolation Of Attacks In Manet Using TS-AOMDV," International Journal of MC Square Scientific Research, vol. 8, no. 1, 2016

[23] W Zhang, S Guo, H Zhang, Y Sui, Y Xue, and Y Xu, Challenging Machine Learning-based Clone Detectors via Semantic-preserving Code Transformations. arXiv preprint arXiv:2111.10793, 2021.

[24] S A Al-Ahmadi, Counterfeit Clones: A Novel Technique for Source and Sink Location Privacy in Wireless Sensor Networks. IEEE Access, vol. 10, 62693-62701, 2022.

[25] T Bonaci, P Lee, L Bushnell, R Poovendran, Distributed clone detection in wireless sensor networks: An optimization approach. In 2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, pp. 1-6. 2011.

[26] J R Dora and K Nemoga, Clone node detection attacks and mitigation mechanisms in static wireless sensor networks. Journal of Cybersecurity and Privacy, vol.1, no.4, 553-579, 2021.

[27] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in Proc. IEEE Symp. Secur. Privacy, pp. 49–63, 2005.