A Trust Based Replica Detection System for Node Replication in Mobile Sensor Networks

P. Edith Linda[1,] R.Sangeetha[2] P.Edreena[3]

Assistant Professor, Department of Computer Science, G.R.Damodaran College of Science, Coimbatore, Tamilnadu[1]
M.Phil Scholar, Department of computer Science, G.R.Damodaran College of Science, Coimbatore, Tamilnadu[2]
Assistant Professor (SG) Department of Computer Science Engineering, Saveetha University Chennai, Tamilnadu[3]

***Abstract*:** *Nowadays, Mobile Wireless Sensor Networks (MWSN) has become most popular and is used to solve challenging problems as industrial sensing and environmental monitoring. MWSN are always ready to be attack by replicas behavior of nodes which would negatively affect the quality of service. Existing schemes in mobile networks incurs efficiency and security problems. In the mobile sensor networks, the node replication attack is a harmful attack where one or more node(s) wrongly claims an identity, are also called clone attack. So, in order to overcome this problem localized algorithms are suggested to resist node replication attacks in mobile sensor networks. The advantages of these algorithms include 1) localized detection; 2) efficiency and effectiveness; 3) network-wide synchronization avoidance; and 4) network-wide revocation avoidance. But the main drawback is high computation complexity and high computation cost. Consequently, the trade-off between security strength and computation overhead has emerged as an area requiring further investigation. So, in order to overcome this trouble an innovative technique is proposed named as Improved Trust based Replica Detection System (ITRDS) which employ clustering algorithm. It is observed that, the proposed scheme decrease the computational complexity, computation cost, computation over head of the network after the detection.*

Keywords: *MWSN, security, Node Replication attack*

I. Introduction:

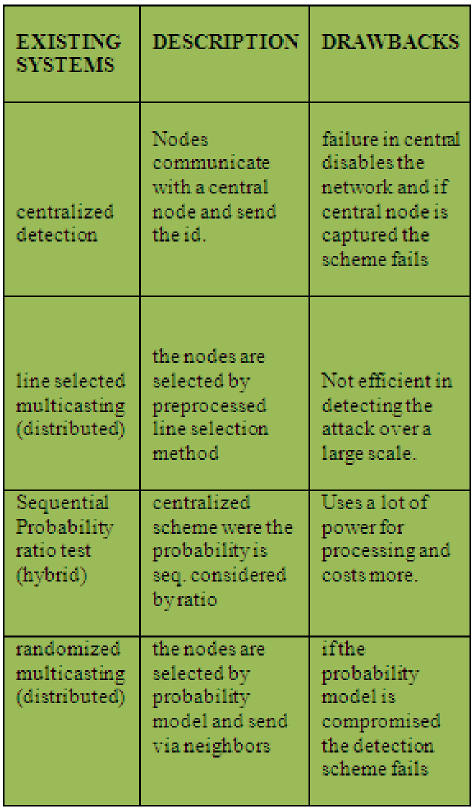
Node Replication Attacks

Sensor networks are used in applications such as environment monitoring and object tracking. Currently, due to the advance in robotics, mobile sensor networks become feasible and applicable. Wireless sensor network (WSN) [4] is networks were the node of the network senses the environment over them. This sensed information is then sent to a base station that is locally located or to a station remotely located. The remote data transfer the data could be received by a local station and can be forwarded by wireless transfer sending the data directly to the remote base station. Wireless sensors consist of two types one is a Stationary Wireless Sensor Network and another is a Mobile Wireless Sensor Network. Stationary Wireless Sensor Network the nodes in the network are static and so cannot move from a place to place. The mobile wireless networks the nodes of the network moves sensing the environment. Mobile sensor network usually used in landscape such as cities for constant sensing of the environment in a given place, it consumes low energy. When sensing remote area and inaccessible places mobile nodes could be used. These provide the safety of the people because they don't have to be physically present in the place of deployment. They can move it remotely. It provides safety and also sensing of critical areas such as volcano epicenters. The wireless transfer of these mobile wireless sensor nodes leads to a susceptibility information theft and information exchange, unauthorized accessing of information, etc. physical attack [11] on the node cannot be prevented easily but most of the time physical destruction nodes is not possible. Thus an attacker attacks the data transmission of the node to destructions the network. There are some general attacks on a mobile WSN [10] are node replication attack, Sybil attack, denial of service attack, wormhole attack, sinkhole attack, etc. Capturing the id, attacking the nodes is the process of the node replication attack and replicating the node ID many times to induce negative information into the network. The existing security mechanisms are incomplete. Hence many techniques are being proposed to detect node replication attack the wireless sensor network.

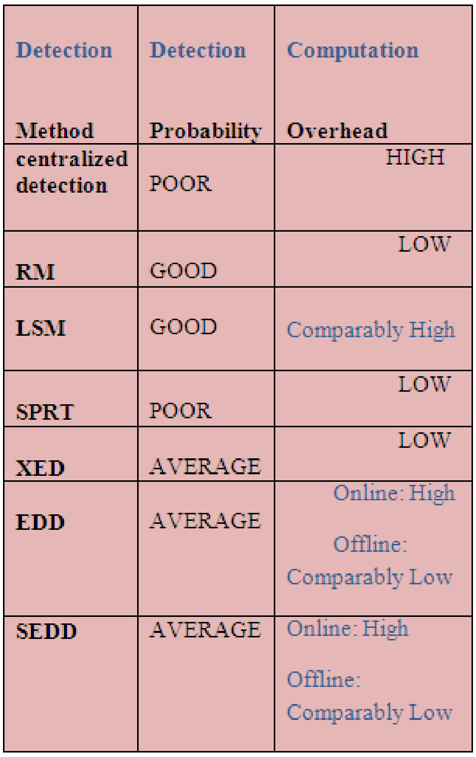
II. Existing Methods:

There are several technologies proposed for detection of node replication attacks the wireless sensor networks. It consists of two types of detection schemes one is centralized and another is distributed [5]. Some of the techniques in distributed are Randomized multicasting and line selected multicasting [14].These algorithms are useful for detection of node replication attack. The centralized detection is more useful for node replication attack in a large scale comprising of the entire network [9]. In two types of the algorithms, those nodes have a secret encrypted ID where the encrypted id is transmitted to the node. In distributed scheme the sender sends the id to the receiver through their nearest nodes [15]. First the receiver will check whether the id is correct or not if the receiver finds the id correct, the next node sends the information to the particular node. If it is not correct then a defensive mechanism is launched.

In case of line selected multicasting, the receiver and the nearest nodes which receive the id are preselected and send. Here the information is encrypted and sent through the nearest the detection of replicas are simplified. If the nearest nodes receive the id correctly the information is forwarded [13].If the nearest nodes do not receive correctly the defensive mechanism is called. The disadvantage is that if there is a large scale attack on the network, the method is not efficient as the attack happens in many places using the same id the nodes located remotely might take the replica for an original node. [1][7][8].In the case of randomized multicasting, the sender and receiver are selected according to the probability model [2]. The probability model will select the nearest node for sending the id. The encrypted id is sent through the nearest node. Here detection can be simple [12]. If the nearest node receives an id not parallel with the model or receives multiple node claims to be the same, the defensive mechanism is revoked. The disadvantage is that if the probability model is known to the attacker, the attacker can replicate the nodes without fear of detection. Other disadvantages are High communication burden and Detect replication attacks. It is very hard to develop the on a large scale .The centralized detection technique is a detection scheme where the nodes in the network send their id to the centralized node so that it can detect the replicas in the node and launch the defense mechanism. This is efficient because it clearly identifies the replicas. But the drawbacks are that the central node if captured will lead to the destruction of the entire network. If the central node is captured, sensed information of the entire network is rendered useless as the attacker can now replicate any number of times without detection. There is also another problem. If the node is failed or destructed, it leads to the failure of detection of entire network henceforth the detection scheme fails. To detect the node replicas in mobile sensor networks, an Efficient and Distributed Detection (EDD) scheme and its variant, SEDD, scheme is proposed. EDD and SEDD possess the following characteristics. 1) Distributed Detection: EDD and SEDD can resist against the node replication attacks in a distributed fashion without involving the base station. 2) Individual Detection: Each node in the EDD and SEDD schemes is able to detect replicas by itself. 3) Cancellation of the replicas can be performed by each
Node without flooding the revocation Messages to the entire network. 4) Efficiency and Effectiveness: The EDD and SEDD schemes can identify the replicas with high detection accuracy. In addition, their communication overhead is only O (1) in the average case but is O (1). There are some drawbacks in this methods are High energy consumption, less performance.



EXISTING SYSTEMS	DESCRIPTION	DRAWBACKS
centralized detection	Nodes communicate with a central node and send the id.	failure in central disables the network and if central node is captured the scheme fails
line selected multicasting (distributed)	the nodes are selected by preprocessed line selection method	Not efficient in detecting the attack over a large scale.
Sequential Probability ratio test (hybrid)	centralized scheme were the probability is seq. considered by ratio	Uses a lot of power for processing and costs more.
randomized multicasting (distributed)	the nodes are selected by probability model and send via neighbors	if the probability model is compromised the detection scheme fails



Detection Method	Detection Probability	Computation Overhead
centralized detection	POOR	HIGH
RM	GOOD	LOW
LSM	GOOD	Comparably High
SPRT	POOR	LOW
XED	AVERAGE	LOW
EDD	AVERAGE	Online: High Offline: Comparably Low
SEDD	AVERAGE	Online: High Offline: Comparably Low

Table: Comparison between various techniques

III. Problem Statement:

In the mobile sensor networks, there is a situation where the adversary can compromise one sensor node, formulate many replicas having the same identity (ID) from the captured node, and locate these replicas back into critical positions in the network for further malicious activities.In the existing research, every node stores security parameter and cryptographic hash function for to check the legitimacy of the nodes. So, there is High computational complexity, High computational cost, High overhead.

Objective of the thesis:

The main intent of the research is to reduce the computational complexity, computational cost, storage overhead and also to improve the security in the wireless sensor networks. Improved Trust based Replica Detection System is proposed which is based on the nodes' identities in the clustered wireless sensor network, which is suitable for such WSNs because it promotes the energy-efficient

The main objective is,

The trade-off between security strength and computation overhead in wireless sensor networks, lower the computational complexity and computational cost and lower the storage overhead.

IV. Proposed Methodlogy:

The methodology that is proposed will be a comprising both central and distributed detection schemes. The mobile wireless network can have a large area for sensing. The area is split into 'clusters'. Thus it is a distributed system. Each sector has a central node were the nodes can send their id for checking. Thus it is also a central in a sector wise analysis. Then as it have both the central and the distributed detection scheme.

In the proposed research, to bring the trade-off between security strength and computation overhead an innovative technique is proposed which is called Improved Trust based Replica Detection System (ITRDS). To the best of our knowledge, we are the first to conduct a systematic study of a trust management system for clustered WSNs from the perspective of both dependability and resource efficiency. The key features of ITRDS go beyond existing approaches in terms of the following aspects:

✓ Cooperations between CMs or between CHs: the indirect trust of a CM is calculated by its CH, within the cluster. Thus it is not essential for each CM to maintain the feedback from other CMs, which will less the communication overhead and eliminate the possibility of a bad-mouthing attack by compromised CMs. The feedback of a CH is enforced a similar manner to obtain the same benefits.

✓ Cooperations between CH: Considering that CHs take on large amounts of data forwarding and communication tasks. The trust evaluating approach is defined for Cooperations between CHs. This method can energetically less the networking consumption while avoiding malicious, selfish, and faulty CHs.

These new designs and other specific features (e.g., independent of any specific routing scheme and platform and so forth) collectively make the ITRDS is a simple, self-adaptive, and dependable solution that can be used in any clustered WSN. The advantages of the methods are less computational complexity, less computational cost, less over head.

V. Conclusion:

The paper has presented study of various node replication attack detection Techniques / protocols for static WSNs. The faster and efficient algorithm can be implemented to overcome the defects in existing systems. The life time of the nodes should be considered and an efficient system can be developed to process of the sensing environment. So, in the proposed system, Improved Trust based Replica Detection System (ITRDS) which employ clustering algorithms. This approach can effectively reduce networking consumption while malicious, selfish, and faulty CHs.

References:

[1]. Distributed Detection of Node Replication Attacks in Sensor Networks, Bryan Parno, Adrian Perrig, Carnegie Mellon University; Virgil Gligor, University of Maryland.

[2]. M. Conti, R.D. Pietro, L.V. Mancini, and A. Mei, "A Randomized,Efficient, and Distributed Protocol for the Detection of NodeReplication Attacks in Wireless Sensor Networks," Proc. ACM MobiHoc, pp. 80-89, Sept. 2007.

[3]. D. Braginsky and D. Estrin. Rumor routing algorithm for sensor networks. In Proceedings of ACM Workshop on Wireless Sensor Networks and Applications, 2002.

[4]. A. Hu and S. D. Servetto. Asymptotically optimal time synchronization in dense sensor networks. In Proceed- ings of ACM International Conference on Wireless Sen- sor Networks and Applications, 2003.

[5]. P. Rohatgi. A compact and fast hybrid signature scheme for multicast packet. In Proceedings of ACM Conference on Computer and Communications Security (CCS), Nov. 1999.

[6]. Choi H, Zhu S, La Porta TF. "SET: Detecting node clones in sensor networks" In: Third International Conference on Security and Privacy in Communications Networks and the Workshops (SecureComm 2007); 2007. p. 341–350

[7]. Zhu B, Addada VGK, Setia S, Jajodia S, Roy S. "Efficient Distributed Detection of Node Replication Attacks in Sensor Networks" In: Twenty-Third "Distributed Detection of Node Replication Attacks resilient to Many Compromised Nodes in Wireless Sensor Networks", 2008 ICST

[8]. Chia-Mu Yu, Chun-Shien Lu and Sy-Yen Kuo, "Efficient distributed and detection of node replication attacks in mobile sensor networks" IEEE 2009.

[9]. Xiaoming Deng, Yan Xiong, and Depin Chen , "Mobility-assisted Detection of the Replication Attacks in Mobile Wireless Sensor Networks" 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications

[10]. V.Manjula and Dr.C.Chellappan, "The Replication Attack in wireless Sensor Networks: Analysis & Defenses" , CCIST 2011, Communications in Computer and Information Science, Volume 132, Advances in Networks and Communications, Part II, Pages 169-178, book chapter, Springer – Verlog.

[11]. M. Conti, R.D. Pietro, L.V. Mancini, and A. Mei, "A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks," Proc. ACM MobiHoc, pp. 80-89, Sept. 2007. [12] B. Parno, A. Perrig, and V.D. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks," Proc. IEEE Symp. Security and Privacy, pp. 49-63, May 2005.

[12]. Jun-Won Ho, Matthew Wright and Sajal 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, June 2011 [15]J. Ho, D. Liu, M. Wright, and S.K. Das, "Distributed Detection of Replicas with Deployment Knowledge in Wireless Sensor Networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1476-1488, Nov. 2009.

[13]. Ms.S.Sharmila "Detection of Node Replication Attack in Mobile wireless Network " An International Journal of Advanced Computer Technology.

[14]. B.Gowtham, S.Sharmila "Location Traced Detection of Node Replication Attack in Mobile Sensor Network"International Journal of Computer Applications, August 2012.

[15]. Moirangthem Marjit Singh " Towards Techniques of Detecting Node Replication Attack in Static wireless sensor networks" International Journal of Information and Computation Technology.ISSN 0974-2239 Volume 4, Number 2 (2014), pp. 153-164.