D.Rajesh Kumar, R.Sathish / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 2, March -April 2013, pp.1111-1115

Mitigation of Replication Attack Detection in Clusters through a Mobile Agent in Wireless Sensor Networks

D.Rajesh Kumar*, R.Sathish**
* (Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam-638 401)
**(Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam-638 401)

ABSTRACT

Among the several other attacks that threatens the security of the Wireless Sensor Networks (WSNs) node replication attack seems to be very harmful ifz present in the network. Replication attack is where an illegitimate node copies the identity of the legitimate node and tries to take hold of the entire network. Node replication attack is also called as clone attack since the clone node also contains the identical copy of information as that of the legitimate node. Most of the times the WSNs tend to operate in clusters. Clustering in sensor networks reduces the number of nodes taking part during the transmission of aggregated data to the data sink. In the existing method usage of mobile agent is one of the approaches for detecting the replicated nodes. But as the size of the network grows larger there should be more than one mobile node involved in the process of detecting the attack, which is not an affordable method. In the proposed method the cluster heads perform this detection job. The information about the nodes are sent to the base station periodically and verified. This paper comes out with a solution for detecting the replicated nodes that joins the cluster. The cluster head is given the additional task of detecting the replicas. An efficient protocol is designed for the cluster head so that it does not require an additional energy and memory requirements.

Keywords – Clone Attack, Clusters, Protocols, Replication Attack, Wireless Sensor Networks

I. INTRODUCTION

A wireless sensor network can be regarded as a collection of nodes that work in a cooperative network. Each and every node is considered to have its own processing capability, memory, power sources, etc. The communication among the nodes takes place in a wireless medium. The applications of sensor networks extend to a wide range from surveillance systems to battle field. There are some basic issues that are to be considered while deploying a sensor network. The first one is the usage of energy resources and next is the security problems.

Wireless Sensor Networks are often prone to various security concerns and loss of resources.

Any compromise in these to basic needs leads to a devastating effect. This effect also leads to the loss of data. In applications such as military, surveillance loss of data leads to the depletion of entire network. The adversaries would try to enter into the network through all the available loop holes. Another constraint is that the security solutions proposed must ensure that it operates with minimal energy resource. WSNs operate through clusters for the better utilization of energy and other resources. In those cases the cluster head takes various additional responsibilities.

Basically sensor networks are prone to three main categories of attacks namely i) Identity Attacks ii) Routing Attacks iii) Network Intrusion.

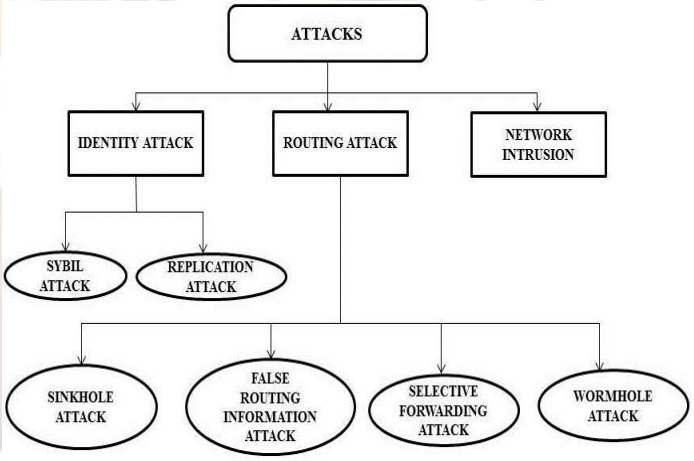


Fig. 1: Categories of attacks in WSNs

Identity attack refers to copying the identities of legitimate node that operating in the network. The categories of identity attack include Replication (clone) attack and Sybil attack. A huge number of identities are forged and fake identities are created by the malicious nodes in the network. These identities are mainly created for disrupting the network protocols.

In routing attack a malicious node is placed in the routing path from source to base station. This aims at tampering the network path or discarding the legal data packets. There are various routing attacks that include wormholes, false routing attack, sinkhole attack and selective forwarding attack. Two

or more malicious nodes in the wormhole attack create a virtual tunnel through which the network traffic is redirected similar to that of a legitimate path. False routing control packets are injected into the network in false routing attack. All the packets that are destined to the base station are influenced by the large spheres that are created by the adversary. In selective forwarding attack the compromised nodes might refuse to forward some selective packets from source to destination in the network.

Network intrusion is where the unauthorized users with less privilege try to get hold of the entire network. These unauthorized users may be external or internal perpetrators.

In this paper we concentrate on one of the identity attack called as replication attack. In this type of attack the legitimate node identity is illegitimately claimed by more than one node. These compromised nodes are further replicated in the whole network. This attack serves as the root for the occurrence of various other attacks such as link layer attack, routing attack, Sybil attack etc. These attacks are commonly referred to as Denial of Services attack. Hence this node replication attack proves to be very dangerous and detection of this attack is very important. There are various centralized and distributed methods available for detecting the replicated nodes, but the problem is the utilization of large amount of memory and energy. For any energy constrained environment like sensor network excess amount of resource usage is a great drawback. Thus it is very important to develop a protocol that satisfies all the constraints.

Rest of the article is organized as follows: Section 2 presents the basic clustering concept and its importance in WSNs; Section 3 comes out with the related works that are available for detecting the replicated attacks; Section 4 comes out with the new protocol for detecting the node replication attack within the clusters; Section 5 presents the simulation results of the protocol; Finally the article is concluded with its future enhancement.

II. CLUSTERING IN WSNS

Sensor nodes normally operate in groups called as clusters for achieving the network scalability. There is a leader associated with each cluster known as cluster-head (CH). There are lots of clustering algorithms available for ad-hoc networks [1-5]. The main objective lies in generating stable clusters with the mobile nodes in the network. Some of the design goals of the WSN include network coverage and longevity. There are various other algorithms for WSN proposed in [6-10] that depends on various factors that include node deployment, network architecture, bootstrapping schemes, network operation model and the CH node characteristics. The CH may either be elected by the sensors in the cluster or it might be assigned by the network designer. The node that is elected as CH might be one of the sensors or the node with rich package of resources.

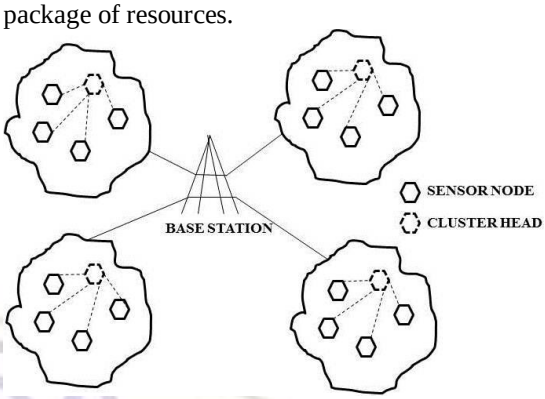


Fig. 2: Sample Cluster Network in WSN

Clustering has a large set of advantages that are listed in the subsequent points. The route set up gets localized within the cluster which results in reduction in the size of the routing table stored by the individual sensor networks. The communication bandwidth can also be conserved through clustering technique as the inter-communication to CH is limited. Also the exchange of redundant messages among the sensor nodes is avoided. The network topology is stabilized through clustering at the sensor level where the topology maintenance overhead is cut.

Optimized management strategies must be implemented in order to improve the network operation. This also helps in enhancing the battery life of the sensors. The CH activities must be scheduled in a cluster such that the nodes can shift to low-power sleep mode when they are not involved in any activity. This results in the reduction of energy conservation. The data collected by the sensor nodes are aggregated by the CH.

III. RELATED WORK

The detection mechanism of replication attack can be classified as prevention and detection schemes. The prevention schemes inhibit the clone node from entering the network. In the identity based method the cryptographic private key are wrapped by both the identities and locations [11]. There are two schemes for detecting the replication attack namely the centralized and distributed protocols.

A centralized protocol [12] is where the control is hold by the central base station (BS). The nodes located within the network send a list of neighbors and their locations to the BS. Next, the BS verifies each and every neighbor list and checks for the presence of the replicated nodes. The base station then forwards an alert message to all the nodes that are present within the network. But this solution faces a single point failure and also incurs a high communication cost. Due to the tunneling effect the nodes that are situated near the base station loose its energy earlier than the nodes that are

situated outer. Another kind of solution for detecting the replication attack is local protocol. The neighboring nodes are made to involve in the voting mechanism. But the drawback of this protocol is that the replicas that are two or more hops away cannot be detected.

There are several distributed protocols available for detecting replication attacks. Every node broadcasts its ID to its neighbor in these protocols. The message forwarded is called as claim and the node that broadcasts the claim is referred to as claimer node. Every node with probability pf on receiving the claim message forwards it to the set of nodes called witnesses. Reporter node is the neighbor node that forwards the claim. If two or more claim messages with same ID are received by the witness node from different locations then the replication attack is detected by the witness node. The protocol in [12] is the first proposed distributed protocol. Randomized Multicast (RM) and Line Select Multicast (LSM) are the distributed protocols that were proposed. The claim message is forwarded randomly to the selected witness node. A set of randomly selected witness nodes receives the claimer node location claim with the probability pf. One of the nodes in the network is likely to receive a conflicting location claim by the neighboring nodes as per the Birthday Paradox prediction methods. Each neighbor is expected to send $O(\sqrt{n})$ messages. The number of sensors in the network is denoted by n. The LSM protocol is similar to that of RM but the difference lies in the detection probability and cost incurred for communication. The location claim forwarded by the neighbor node is broadcasted to all the other nodes with the probability of pf. The neighbor node randomly selects fixed number of g witness nodes and the signed claim is sent to all the g nodes. The number of witness nodes g is smaller when compared to RM. The nodes that are routing the claim message should check the signature of the claim and the signed claims are to be stored. Finally the claims that are stored within the same iteration is checked for coherence. Hence the forwarding nodes of the claim are also considered as the claimer node. If the intersection of the route paths of the nodes that originate from different locations occur then node replication is likely to be detected.

Two other protocols namely SDC and P-MPC are proposed in [13]. In this protocol study the network is considered as a geographic grid. In SDC protocol a node's identity is randomly mapped to one of the cells in the grid with the help of unique geographic hash function. The location claim message is further forwarded to the mapping cell. The location claim is flooded within the cell once the first copy of the location claim arrives at the destination cell. The nodes in the cell are randomly selected as the witness nodes. In P-MPC, a node's identity is mapped to several cells in the grid in order to increase the reliability. The witnesses can be predicted by the attackers with the help of predefined locations or cells.

Another efficient and distributed protocol was proposed in [14, 15]. This protocol is different from that of RM and LSM. In RED the claimer node α chooses the same witness nodes g, but in RM and LSM the reporter node randomly chooses the set of witness nodes. The witness nodes' locations are determined with the claimer node ID and seed rand in RED. In each iteration the seed is broadcasted by the trusted entity to the entire network. The seed value changes keeps changing in each of the detect iteration and hence it becomes difficult for the attackers to forestall the witness nodes. The claimer node of each neighbor node with the probability pf is accepted as the reporter node and then the claim message is forwarded to g witness nodes. A higher success rate is detected as the pf gets larger and the claimer node has more number of reporter nodes.

A strategy that avoids the prediction of critical witness by the attackers is proposed in Randomwalk [16]. Here the protocol distributes the charge of witness node selection to the passed nodes of random walks and hence the chance of finding the witness nodes by the adversaries is very less. For each node a, this protocol RAndom WaLk (RAWL) starts several random walk randomly and then the witness nodes of node a is selected from the passed nodes. From the algorithm analysis it is seen $O(\sqrt{n} \log n)$ walk steps are sufficient for detecting the replication node with a great probability. Next is the Table-assisted RAndom WaLk (TRAWL) which is based on RAWL protocol. In this protocol for reducing the memory cost each node is added with trace table. Basically the memory cost is incurred because of storing location claims; whereas in TRAWL each node stores O(1) location claims, the size of the trace table is $O(\sqrt{n} \log n)$.

Randomness is considered as an important criterion for finding the witness that is proposed in [17, 18]. This method avoids the prediction of future witnesses. In case the attacker could predict the future witnesses then it is possible for the attackers to subvert the node. If this situation occurs then the replicated node may go undetected.

IV. PROPOSED WORK

The proposed protocol deals with detecting the replication node in the network. The well-known existing LEACH (Low Energy Adaptive Clustering Hierarchy) protocol is implemented for clustering process. Further a detection protocol is developed for detecting the clone node. A mobile agent is made to monitor the network with time intervals. Following section provide the brief description about the LEACH protocol and the replication detection protocol.

1.1 LEACH

The first hierarchical cluster-based routing protocol developed was LEACH protocol. The nodes are partitioned into clusters and the node with additional privileges is selected as Cluster Head (CH). Cluster Head is responsible for aggregating the data sending it to base station from the nodes. There are two phases in LEACH protocol implementation.

- **Set-up Phase**: The CH election process is carried out in this phase. Once the node becomes CH an advertisement packet is sent to the neighbors stating its selection as the CH.
- **Steady-state Phase**: Transmission of data begins in this phase. The data are sent by the nodes during the allocated time slots. Minimal energy is used for transmitting the data. Once the data from all the nodes are received the CH sends the data to the BS after the aggregation of data is complete.

Even then LEACH protocol suffers from various drawbacks, for time being this protocol is used for clustering the sensor nodes. The major contribution is given for the development of the clone node detection algorithm.

1.2 REPLICATION ATTACK DETECTION ALGORITHM (RAD)

As discussed earlier clone attack proves to be very dangerous since it leads to various other identity attacks. Hence detecting replication attack is very important. The pseudo code for RAD protocol is given below:

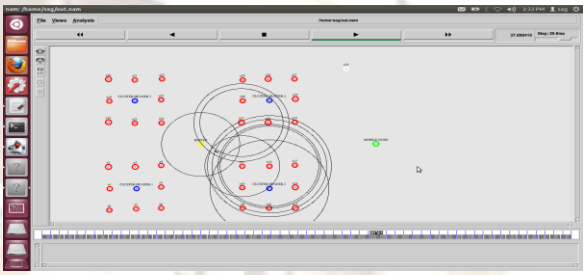
Algorithm: RAD protocol
Input: n, C_1…….. C_i
Output: Legitimate node=0, Replicated Code=1

```
1.  Procedure cluster(n)
2.      LEACH( );
3.      for i=0 to n then
4.          return C1…….. Ci
5.      end for
6.  end cluster
7.  Procedure RAD(n, C1…….. Ci)
8.      if (n joins the cluster)  then
9.          Cluster(n);
10.     end if
11.     L ← Location Claim of n
12.     id ← node id
13.     info ← M(L, time, Ci, id)
14.     detect(L, info, id)
15. end RAD
16. Procedure detect(L, info, id)
17.     if (MA info & CH info are similar) then
18.         return 0
19.     else if  (Ci info equals Cn info) then
20.         return 1
21.     end if
22. end detect
```

In the above algorithm the cluster formation is implemented with LEACH protocol. The cluster head is responsible for collecting the node information. In addition to the cluster head a Mobile Agent (MA) also keeps a record of the node information. At regular interval of time the CH information and the MA information are verified. The information consists of each node's location claim, timestamp, ID etc. If any node shows different location claim at the same time then the clone is detected. This protocol can be added under distributed detection cadre.

V. SIMULATION RESULTS

The simulation is performed in NS2 simulator. The number of nodes ranges from 25 to 150. The coverage area that is been set is 1000x1000. Following screen shots shows the simulation result. The result includes the formation of clusters and the detection of clone node.



. Fig. 3: Sensor Nodes grouped into clusters

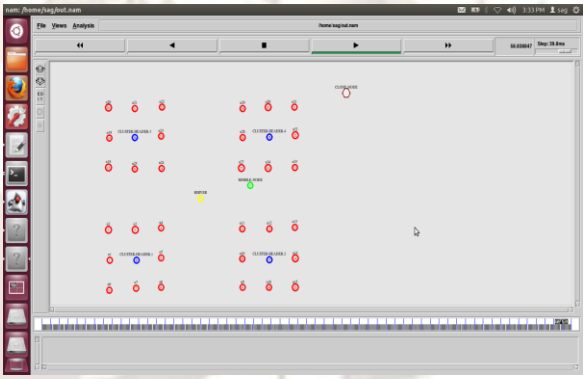


Fig. 4: Replication attack detected

The following chart provides the detection accuracy for different number of nodes. The detection accuracy falls as the number of sensor nodes increase. The protocol is to be enhanced for detecting the replication attack effectively.

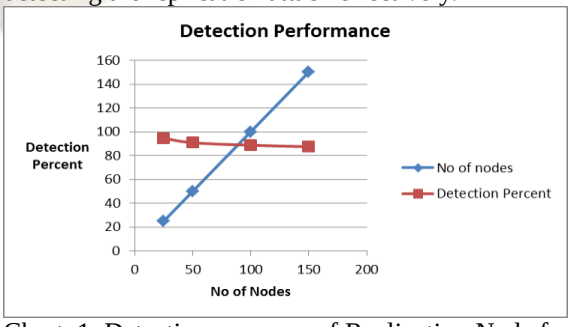


Chart. 1: Detection accuracy of Replication Node for various no of nodes

VI. CONCLUSION

Basically the existing approaches for detecting clone attack depend on a static network model without any global solution. Many other methods detect the attack accurately but incur heavy communication cost, energy consumption. In the proposed solution the sensor nodes work in clusters which minimize the energy consumption. At the same time the detection protocol is implemented with less communication cost as the information comparison happens at regular interval between the MA and the CH. Base station remains silent and does not have any active participation. In the future enhancement it is important to perform clustering process even more effectively and also increase the detection accuracy. The detection rate is to be improved as the number of sensor nodes in the network increases.

REFERENCES

[1] V. Kawadia, P.R. Kumar, Power control and clustering in Ad Hoc networks, in: *Proceedings of IEEE INFOCOM, San Francisco, CA, March 2003.*

[2] M. Chatterjee, S.K. Das, D. Turgut, WCA: a Weighted Clustering Algorithm for mobile Ad Hoc networks, *Cluster Computing 5 (2) (2002) 193–204.*

[3] A.D. Amis, R. Prakash, T.H.P. Vuong, D.T. Huynh, Max-Min Dcluster formation in wireless Ad Hoc networks, *in: Proceedings of IEEE INFOCOM, March 2000.*

[4] A.B. McDonald, T. Znati, A mobility based framework for adaptive clustering in wireless ad-hoc networks, *IEEE Journal on Selected Areas in Communications 17 (8) (1999) 1466–1487.*

[5] S. Basagni, Distributed clustering algorithm for ad-hoc networks, *in: Proceedings of the International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN), Fremantle, Australia, June 1999.*

[6] G. Gupta, M. Younis, Load-balanced clustering in wireless sensor networks, *in: Proceedings of the International Conference on Communication (ICC 2003), Anchorage, Alaska, May 2003.*

[7] S. Bandyopadhyay, E. Coyle, An energy efficient hierarchical clustering algorithm for wireless sensor networks, *in: Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), San Francisco, California, April 2003.*

[8] S. Ghiasi, A. Srivastava, X. Yang, M. Sarrafzadeh, Optimal energy aware clustering in sensor networks, *Sensors Magazine MDPI 1 (1) (2004) 258–269.*

[9] O. Younis, S. Fahmy, HEED: A Hybrid, Energy-Efficient, Distributed clustering approach for Ad Hoc sensor networks, *IEEE Transactions on Mobile Computing 3 (4) (2004) 366–379.*

[10] W.B. Heinzelman, A.P. Chandrakasan, H. Balakrishnan, Application specific protocol architecture for wireless microsensor networks, *IEEE Transactions on Wireless Networking (2002).*

[11] Brooks R, Govindaraju PY, Pirretti M, Vijaykrishnan N, Kandemir MT.(2007), On the Detection of Clones in Sensor Networks Using Random Key Predistribution, *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews.;37(6):1246–1258.*

[12] Parno B, Perrig A, Gligor V, Distributed Detection of Node Replication Attacks inSensor Networks, *Proceedings of the IEEE Symposium on Security and Privacy; 2005, p. 49 – 63.*

[13] S. Zhu, S. Setia, and S. Jajodia, LEAP: efficient security mechanisms for large-scale distributed sensor networks, *in Proc. 10th ACM Conf. on Computer and Communications Security (CCS '03), 2003, pp. 62–72.*

[14] M. Conti, R. Di Pietro, L.V. Mancini, and A. Mei, A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks, *2007, In ACM MobiHoc, pages 80–89.*

[15] M. Conti, R. Di Pietro, L.V. Mancini, and A. Mei, Distributed Detection of Clone Attacks, *IEEE Transactions on Dependable and Secure Computing, 2010.*

[16] Yingpei Zeng, Jiannong Cao, Senior Member, IEEE, Shigeng Zhang, Shanqing Guo and Li Xie, Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks, *IEEE Journal on Selected Areas in Communications, 2010, pages 677-691 Vol. 28, No. 5.*

[17] V.Manjula, C.Chellappan, Replication Attack Mitigations for Static and Mobile WSN, *International Journal of Network Security and Its Applications (IJNSA), 2011, vol.3, No.2.*

[18] V.Manjula, C.Chellappan, The Replication Attack in wireless Sensor Networks: Analysis & Defenses, *CCIST 2011 Communications in Computer and Information Science, 1, Volume 132, Advances in Networks and Communications, Part II, 2011, Pages 169-178, book chapter, Springer –Verlog.*