ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

Randomly Directed Exploration Protocol for Clone Detection in Wireless Sensor Networks

P.Hima Bindu[1], T. Venkata Naga Jayudu[2]

Intell Engineering College (Affliated to JNTU-Ananthapuramu & Approved by AICTE and Accrediated by NBA),Ananthapuramu, Andra Pradesh, India

Intell Engineering College (Affliated to JNTU-Ananthapuramu & Approved by AICTE and Accrediated by NBA),Ananthapuramu, Andra Pradesh, India

ABSTRACT: Wireless sensor networks are resource constrained and vulnerable to various kinds of attacks. In this paper we study node clone attack. Many solutions came into existence and for detecting this attack. Many solutions need assumptions to have the problem solved in large-scale deployment of sensors. They have tradeoffs between the solutions provided and network conditions. Recently Li and Gong proposed two protocols for node clone detection with different tradeoffs with network conditions. Distributed Hash Table (DHT) was used to have distributed mechanisms for node clone detection. Due to the overhead caused by DHT, they proposed another protocol that overcomes this problem. In this paper, we implement a novel mechanism that can detect node clone attack in wireless sensor networks. We made simulations in NS2 to demonstrate the proof of concept.

KEYWORDS:Wireless sensor networks, node clone detection, distributed hash code

I. INTRODUCTION

Wireless sensor networks became very useful networks in the real world as they are easy to deploy and useful for monitoring various environments in both civilian and military contexts. Due to the popularity of WSN, there are increased security threats. The general structure of WSN and its sensor and base station nodes is as presented in Figure 1.

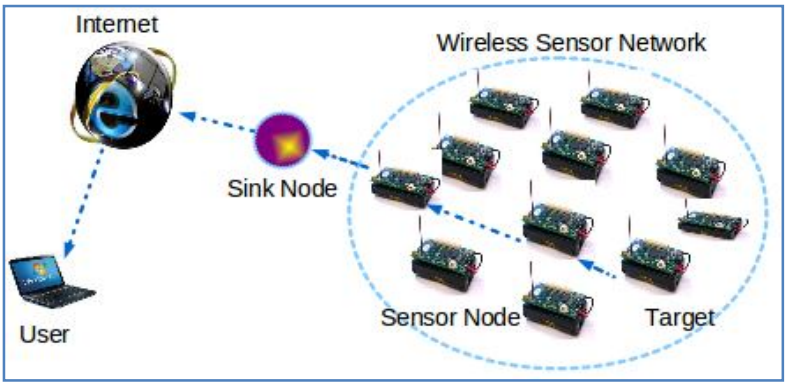

Fig. 1 – Typical wireless sensor network

As can be shown in Figure 1, wireless sensor network is a collection of sensor nodes which can sense data about targets. The sensor nodes sense the unknown object data and send to sink node. The sink node can be accessed by authorized users through Internet. In fact the sink node can be queried in order to monitor the area under coverage of WSN.

Node cloning is one of the attacks in WSN that will cause the network to lose sensitive information to adversaries. There were many node clone detection mechanism found in the literature. The solutions are classified into

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

prevention mechanism, centralized mechanism and distributed mechanisms. More details can be found in section II. In this paper, we built a framework and proposed an algorithm in order to detect node clone attack sin WSN. The remainder of the paper is structured as follows. Section II provides review of literature on prior works. Section III presents the proposed solution. Section IV provides details of experiments while section V concludes the paper besides making directions for future work.

II. RELATED WORKS

The literature on node clone detection is reviewed and presented in this section. The prior works in node clone detection in WSN reveal prevention mechanisms, centralized detection and distribution detection models. With respect to distributed detection model [1] it is evident that every node in WSN has the capabilities to detect node clones. Two probabilistic protocols were explored in [1] to achieve this. However, it has many assumptions that will limit the practical use of the detection mechanism in the real world. Other clone detection mechanisms were explored in [7] and [6] where nodes have the knowledge of the geography where the nodes have been deployed. Various protocols have different requirements including neighbors' information, awareness of all nodes, knowledge of network geography, DHT nodes information.

With respect to centralized detection the detection process is with the base station. The sensor nodes will not have the capabilities of node clone detection. It also causes communication cost. The SET protocol explored in [8] is able to reduce communication cost by using the notion of constructing exclusive subsets. In [9] another solution is proposed using the notion of pre-key distribution as explored in [10] technically it is the process of detecting the compromised keys instead of detecting clone nodes. As per this protocol, each and every node exports its keys to base station. A problem with this kind of approach is the high rate of false positive and false negative reports.

With respect to prevention mechanisms, location based keys are explored in [3] for node clone detection process. Identity based cryptography is used in order to achieve this. The location based keys are issues by trusted agents by travelling the WSN. Similar kinds of solutions are made in [5] and [4]. These are useful in specific WSN applications in the real world. However, the assumptions they have will have limits in real time applications.

III. PROPOSED SOLUTION

In this paper we proposed a solution that can detect node clone attacks in WSN. We built a general framework that has underlying algorithm in order to ensure that the node clone attacks launched by adversaries are detected positively. The general framework is as shown in Figure 2. Then we proposed an algorithm named **Randomly Directed Exploration Protocol for Clone Detection** for node clone detection.

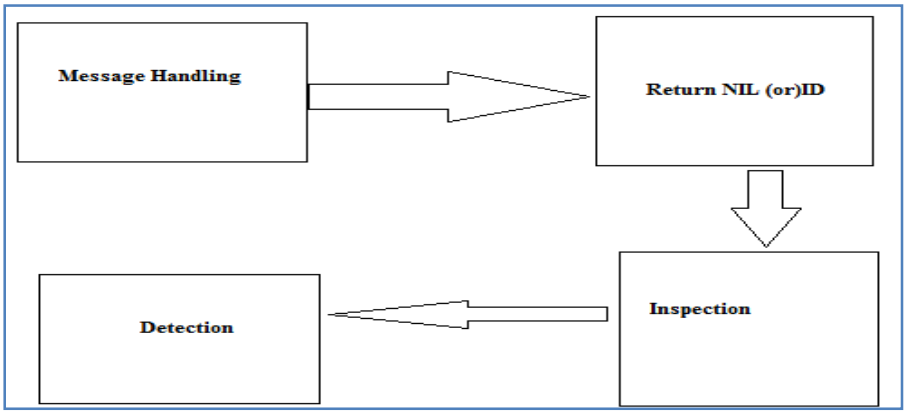

Figure 2 – Overview of node clone detection process

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

As can be seen in Figure 2, there is outline of the node clone detection process. First of all the message handling phase is called out. When the message arrives at its destination, the underlying algorithm is supposed behave based on the return messages. The algorithm returns NIL when message arrives at the destination otherwise it returns the ID of the node and the algorithm continues. The other phases in the proposed solution include inspection and detection. The inspection phase is used to determine whether there is possible detection and the actual detection phase confirms the clone presence in the WSN. The proposed algorithm is as shown in listing 1.

```
Algorithm: Randomly Directed Exploration
Inputs   : Message
Outputs  : NIL, or ID of node and detection result

1 Finding key
2 Check key and return NIL or ID
3 FOR ALL NODES IN WSN
      If key belongs to key set then
         Perform inspection
      End if
INSPECTION PHASE
4 verify signature
5 check in cache table
6 if found in two locations
     Confirm clone detection
     Broadcast the proof
7 else
      Save the details to cache table
9 end
```

Listing 1 – Node clone detection algorithm

As can be seen in listing 1 there is evidence of detecting clones in the verification phase followed by detection process. The node clone detection procedure initially return NIL or ID based on the arrived message. When there is key verification and suspects duplicate, then verification phase is carried out in order to check in cache and update the cache accordingly and broadcast the evidence of the node clone if found positively.

A. Load Balancing and Traffic Distribution

Apart from node clone detection, we implemented load balancing and traffic distribution mechanisms that work towards reducing congestion and improving throughput. Mobile nodes act as transmitter and receiver of data and they are utilized in such a way that information can be updated even when the nodes are out of range. This is achieved via cooperatitve transmission of data. Nodes are also able to compute distance range from node to node thus nodes can sense and update information. Load balancing has other advantages such as energy efficiency besides improving throughput and reducing congestion. The experimental results are shown in the following section.

IV. EXPERIMENTAL RESULTS

Experiments are made through NS2 simulations. The simulations demonstrate the wireless sensor network with base station and sensor nodes. Besides it shows how the node clone attack is made and detected by the proposed solution. Malicious nodes are detected and secure communications are in place using asymmetric cryptography. The experiments are made in terms of number of nodes and average number of messages sent per node; number of nodes and detection probability; packet delivery ratio and time; number of nodes and transactions per second. The performance of the proposed system is compared with the existing system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

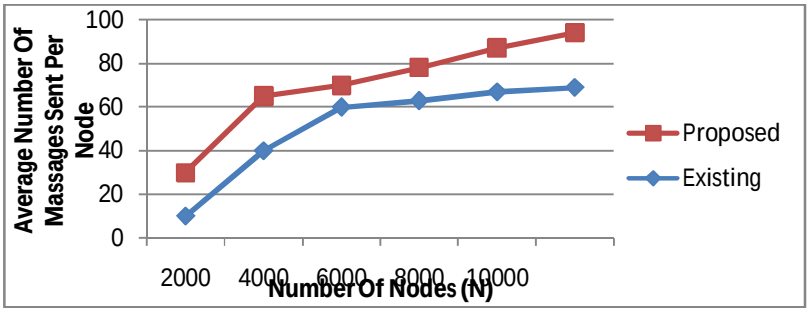

Figure 3 – Number of messages sent per node

As can be seen in Figure 3, it is evident that the proposed system outperforms existing system in terms of average number of messages sent per node.

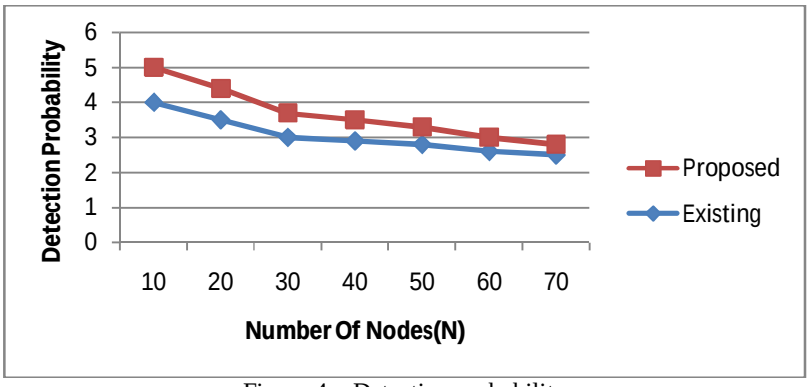

Figure 4 – Detection probability

As can be seen in Figure 4, it is shown that the number of nodes have influence on the detection probability. The proposed system exhibits higher detection probability.

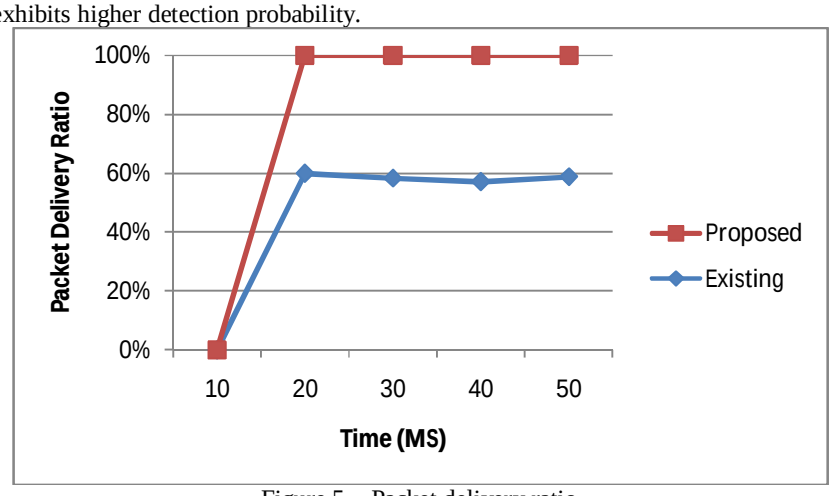

Figure 5 – Packet delivery ratio

As can be seen in Figure 5, the packet delivery ratio is compared between the existing and proposed systems. The proposed solution has increased the packet delivery ratio.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

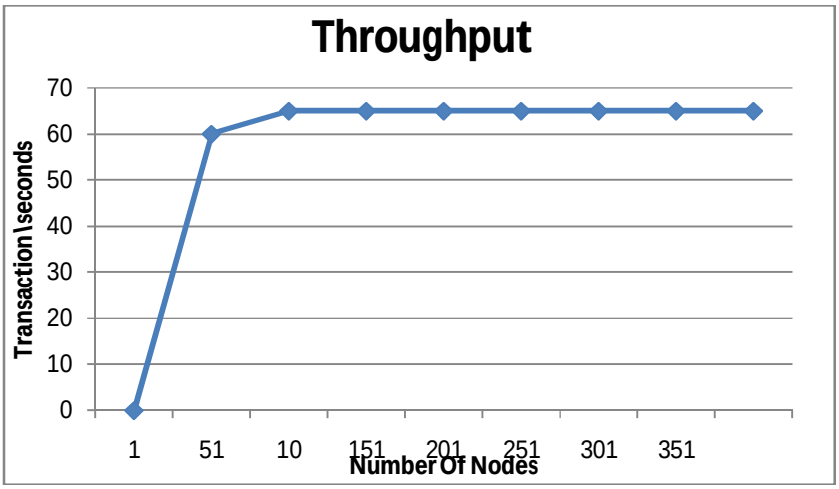

Figure 6 – Throughput performance

As can be seen in Figure 6, it is evident that the throughput of the proposed system is better than that of existing system.

V. CONCLUSIONS AND FUTURE WORK

In this paper we studied the node clone detection attacks and counter measures in WSN. Node clone attack is one of the attacks in WSN that exploit vulnerabilities in order to obtain sensitive information from the network. An adversary can launch such attack and makes a clone node for a genuine sensor node. Since the clone node is under the influence of the adversary, it follows the instructions of the attacker. Thus it collected sensitive information flows that can benefit adversary in one way or other. We proposed an algorithm that has mechanisms to detect clone attacks in WSN. The algorithm acts as inspector that will monitor messages and in order to determine node clone attacks. We built a simulation model which demonstrates the proof of concept. The NS2 simulations reveal that the proposed solution is useful to detect clone attacks in WSN. In future we would like to implement the algorithm in real world environment.

REFERENCES

[1] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proc. IEEE Symp. Security Privacy*, 2005, pp. 49–63.
[2] H. Balakrishnan, M. F. Kaashoek, D. Karger, R. Morris, and I. Stoica, "Looking up data in P2P systems," *Commun. ACM*, vol. 46, no. 2, pp. 43–48, 2003.
[3] Y. Zhang,W. Liu,W. Lou, andY. Fang, "Location-based compromisetolerant security mechanisms for wireless sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 247–260, Feb. 2006.
[4] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in *Proc. 10th ACM CCS*, Washington, DC, 2003, pp. 62–72.
[5] R. Anderson, H. Chan, and A. Perrig, "Key infection: Smart trust for smart dust," in *Proc. 12th IEEE ICNP*, 2004, pp. 206–215.
[6] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks inwireless sensor networks," in *Proc. 8thACMMobiHoc*,Montreal,QC, Canada, 2007, pp. 80–89.
[7] B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient distributed detection of node replication attacks in sensor networks," in *Proc. 23rd ACSAC*, 2007, pp. 257–267.
[8] H. Choi, S. Zhu, and T. F. La Porta, "SET: Detecting node clones in sensor networks," in *Proc. 3rd SecureComm*, 2007, pp. 341–350.
[9] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," *IEEE Trans. Syst.s, Man, Cybern. C,Appl. Rev.*, vol. 37, no. 6, pp. 1246–1258, Nov. 2007.
[10] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. 9th ACM Conf. Comput. Commun. Security*, Washington, DC, 2002, pp. 41–47.

[11] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. CRYPTO*, 1984, LNCS 196, pp. 47–53.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

[12] R. Poovendran, C. Wang, and S. Roy, *Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks*. New York: Springer-Verlag, 2007.
[13] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.
[14] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Schenker, "A scalable content-addressable network," in *Proc. SIGCOMM*, San Diego, CA, 2001, pp. 161–172.
[15] I. Stoica, R.Morris, D. Liben-Nowell, D. R. Karger,M. F.Kaashoek, F. Dabek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup protocol for internet applications," *IEEE/ACM Trans. Netw.*, vol. 11, no. 1, pp. 17–32, Feb. 2003.
[16] A. I. T. Rowstron and P. Druschel, "Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems," in *Proc. IFIP/ACM Int. Conf. Distrib. Syst. Platforms Heidelberg*, 2001, pp. 329–350.
[17] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in *Proc. 1st Int. Conf. Simulation Tools Tech. Commun., Netw. Syst. Workshops*, Marseille, France, 2008, pp. 1–10.
[18] A. Awad, C. Sommer, R. German, and F. Dressler, "Virtual cord protocol (VCP): A flexible DHT-like routing service for sensor networks,"in *Proc. 5th IEEE MASS*, 2008, pp. 133–142.
[19] R. Diestel, *Graph Theory*, 3rd ed. New York: Springer, 2006

BIOGRAPHY

T. Venkata Naga Jayudu, received his B.Tech degree in Computer Science and Information Technology from Jawaharlal Nehru Technological University, Hyderabad, India, in 2005. Received M.Tech degree in computer science at Jawaharlal Nehru Technological University, Anantapur, India, in 2011. He is an Asst.Professor at INTELL Engineering college, Anantapur, India. He published papers in various national and international journals. His interesting research area is Mobile Ad-Hoc Networks, Network Security and wireless sensor networks.

P.Hima Bindu, received her B.Tech degree in Information Technology from Jawaharlal Nehru Technological University, Anantapur, India, in 2012.