© 2015 IJSRSET | Volume 1 | Issue 4 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Agent Based Security Framework towards Misrouting Attack in Wireless Sensor Networks under Node Replication

Rama Chaithanya Tanguturi*[1], C. Jayakumar[2]
*[1]Department of Computer Science and Engineering, Anna University, Chennai, Tamil Nadu, India
[2]Department of computer Science and Engineering, R.M.K Engineering College, Chennai, Tamil Nadu, India

ABSTRACT

Drastic development in wireless technology increased the demand for Wireless Sensor Network (WSN) applications for monitoring areas of interest. The sensible information monitored by the sensor nodes need to be securely communicated to the sink. Even after the evolution of mobility in the wireless sensor networks, a large number of application deploying static nodes. Node replication in WSN gives the attacker a chance to perform various attacks. One of the major attacks in this category was misrouting attack. The replicated node changes the route of the non-captures nodes resulting entire network compromise. We proposed an agent based security frame work which makes the non-captures nodes will not affected by the captures nodes thereby increase the resilience of the network under misrouting attack.

Keywords: Wireless Sensor Networks, Security, Misrouting, Node Replication, Agent

I. INTRODUCTION

In the current scenario, Wireless sensor networks consists of wirelessly communicating sensor nodes which monitors the surrounding environments producing data corresponding to the area of interest and forwarding to a collection points called sink or base station through intermediate nodes or access points.

Wireless Sensor networks are resource constrained networks with limited power supply (Battery), low computational capacity and short range of wireless communicating device. As sensor nodes carry critical information secure communications need to be ensured, because these networks are prone to attacks. Energy is the critical constraint for WSNs. All the applications need to consider the energy level of the nodes for their operations.

A security frame work for WSN defines the method of protecting sensor network from the attacks. WSNs require a special category of security mechanism comprising a simple and secure mechanism which ensures secure communication to entire network. Replication attack is highly potential attack where attacker tries to capture a fraction of the nodes in the network and will extract the key pool information and start communicating with the other parts of the network [1]. Once the attacker reaches a threshold value of the captured nodes entire network will be retrieved by the attacker. In this paper we focus on the most serious misrouting attack introduces by capturing and replicating a single or fraction of nodes in static wireless sensor networks. The works in [2] - [7] detail different mechanisms to increase the resilience of the network.

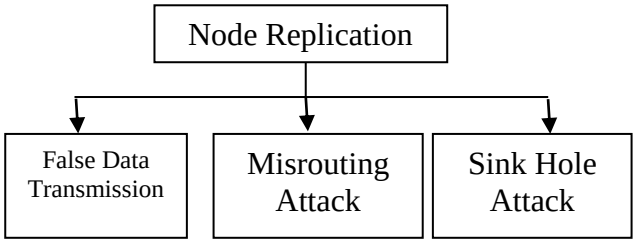

Figure 1: Effect of node replication

Figure 1 show the various possible attacks based on node replication by a smart adversary. The remainder of

the paper is as follows, section II details the attack model, section III elaborates the related works and section IV proposed frame work.

The organization of this paper is as follows. In Section 2 (**Methods and Material**), details of the proposed scheme. In Section 3 (**Result and Discussion**), the proposed model is analysed and evaluated and conclusion in the section 4.

II. METHODS AND MATERIAL

Attack Model

The advance in the wireless technology eases mobility in the wireless sensor networks. Even after the emergence of mobility in the wireless sensor networks, majority of the applications deploying static sensor nodes. These nodes are unattended and targeted by the intruder for getting control over the entire network. Intruder will gather information by listening to the network traffic and uses the same for node capture. Once intruder succeed in node capture, will invoke the node replication procedure as follows:

Procedure for node replication:

1. Intruder will get the captured node ID's
2. Extract Key shares available in the captured node
3. Draw the pair-wise keys used by the captured node
4. Capture more nodes
5. Introduce new node in the network with captures node ID and Keying information

Intruder introduces replicated nodes to perform various attacks such as misrouting, false data transmission etc. easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

Related Works

A witness based replication detection scheme was proposed in [8] where the collective action of multiple nodes with the network topology is used to detect the replicated nodes in the wireless sensor network. The randomized multicast uses randomly selected witness nodes to have node identities which detect multiple claims of a node at different locations. Line select multicast considers the intersection of claims at some point in the routing path of the nodes. A recent work in [9] is a self-healing, Randomized, Efficient, and Distributed (RED) protocol which considerably increases the resilience to a smart adversary when compared with the protocols proposed in [1], the witness in this protocol may present anywhere in the network. The adversary has to clone all these distributed nodes to escape from the replication detection, protocol need an infrastructure to distribute pseudo-random number. A memory efficient protocol in [10] using public key cryptographic scheme for replication detection. A periodic check based scheme SET in [11] gathers node identities periodically up the network and detect the replicated nodes with conflict of identities at a central point. Two Localized Multicast approaches in [12], Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC) which maps the node identities to single and multiple grids in the network, by analysing the identities the replication is detected.

Proposed Method

This framework introduces a mobile agent in the network to carry out the secure operations and also to identify the node capture and node replication attacks. Mobile agent is a piece of software code that can reside in any node or clones in to the other node with desired configuration which can handle any critical situations. By using software agent this framework will never trade-off on the network resources which caused by the operation of the proposed mechanism. Mobile agent in the network will resides in the required node shown in figure. 4.1. Depending up on the requirement of the network, the agent will be configured. Mobile agent will take necessary action in the wireless sensor network. As we assumed the network as a static one, the nodes once deployed will not move from the location of deployment. Assume that, Time required for nodes to get the path establishment in the network is Te, Time required for the intruder to launch node capture attack is Ti. Here Ti >> Te because immediate after the establishment of the network the nodes start establishing the paths with the adjacent nodes and the sink. So, we consider the time for the intruder to launch the attack will be greater than the time for link establishment. Once after the deployment of the network nodes will have routing table which is used to forward the sensed data to the sink. The mobile agent will clone to the nodes in the network and copies

all the routing information to the database. Due to the static nature of the nodes the routing table will not be changed unless a node misbehaves in the network.

III. RESULTS AND DISCUSSION

The framework will be explained with a wireless sensor network randomly deployed in an area of interest like battle field as shown in figure.2

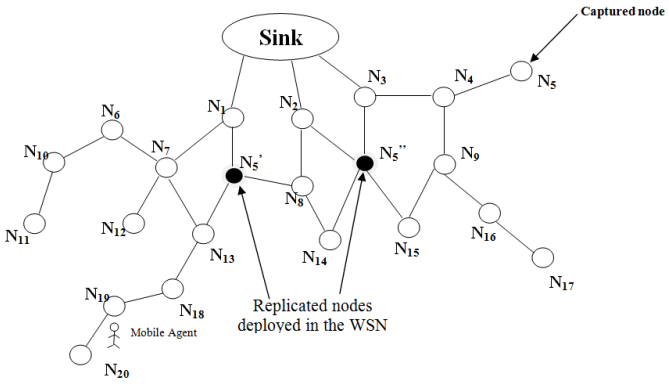

Figure 2 : Wireless Sensor Network randomly deployed in an area of interest

The route for each node towards the destination after the deployment of the network is as show in Table I. Intruder captures the node N_5 and replicated in two places with same node ID N_5 as show in fig.1.

TABLE I
NODE TRUSTED ROUTE TABLE

Node	Trusted Route To Destination	Node	Trusted Route To Destination
N_1	Direct communication with sink	N_{11}	< N_{10} ,N_6, N_7 ,N_1>
N_2	Direct communication with sink	N_{12}	< N_7 ,N_1>
N_3	Direct communication with sink	N_{13}	< N_7 ,N_1>
N_4	<N_3>	N_{14}	< N_8 ,N_2>
N_5	< N_4, N_3>	N_{15}	< N_9 ,N_4 , N_3>
N_6	< N_7, N_1>	N_{16}	< N_9 ,N_4 , N_3 >
N_7	<N_1>	N_{17}	< N_{16},N_9 ,N_4 , N_3>
N_8	<N_2>	N_{18}	< N_{13} ,N_7 , N_1>
N_9	< N_4 ,N_3>	N_{19}	< N_{18}, N_{13} ,N_7 , N_1>
N_{10}	< N_6 ,N_7 , N_1>	N_{20}	<N_{19} , N_{18}, N_{13} ,N_7 , N_1>

The replicated nodes will request neighbour nodes to change their routes towards their destination. Making the nodes believe that the route through replicated node will be the correct path towards the destination. In this framework every node has to coordinate with the mobile agent to update route towards the destination. The WSN will act similar to the WSN without the implementing the framework unless a route request reaches the agent. Once a route request reaches the agent, it compares the trusted route RT with the new requested route RR to find from which hop the route is bypassed. Agent will list the nodes that are having the bypassed node as first hop in their route and check whether these nodes also communicated for route request. The replicated nodes will request neighbour nodes to change their routes towards their destination. Making the nodes believe that the route through replicated node will be the correct path towards the destination. In this framework every node has to coordinate with the mobile agent to update route towards the destination. The WSN will act similar to the WSN without the implementing the framework unless a route request reaches the agent. Once a route request reaches the agent, it compares the trusted route RT with the new requested route RR to find from which hop the route is bypassed. Agent will list the nodes that are having the bypassed node as first hop in their route and check whether these nodes also communicated for route request. If all the first hop nodes route request reaches the agent then the bypassed node will be considered as failure node else the new route request is due to some replicated nodes introduces by the intruder. In the above example the intruder captured the node N5 and replicated it in two different places in the network. The replicated node N5 will communicate with its neighbour as a trusted next hop towards the destination. The nodes will calculate the new path and requests the mobile agent which route to choose to have secure communication. The requests for route change are shown in Table II.

TABLE II

NEW ROUTE REQUEST

New route requested nodes (S_N)	**N_8, N_{13} , N_{14} , N_{15}, N_{18} , N_{19} , N_{20}**

TABLE III
N_7 FIRST HOP NODES

Nodes with N7 as first hop towards sink (S_F)	**N_6, N_{12} , N_{13}**

The new route request come from node N20 is as follows < N19, N18, N13, N5, N1>.When comparing it with the trusted route, node N7 is bypassed in the new request. From the Table I the nodes having N7 as first

hop towards the destination are as shown in Table III. Let SF be the set of first hop nodes of N7 and SN be the set of nodes that requested for route request. As shown in fig 3 if SF ⊆ SN new route will be selected else replication nodes present in the network.

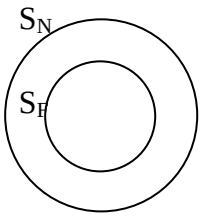

Figure. 3 : $S_F \subseteq S_N$

Out of one hop distance nodes N6, N12, N13 of N7 only N13 requested for route change. From this the agent will identify that the node N7 is a legitimate node towards the destination by discarding the new route request from the node N20. Mobile agent identifies the node N5' as a replicated node and flooded the information into the network.

IV.CONCLUSION

We proposed a security framework for the misrouting attack in the wireless sensor network under replication attack. The analysis shows that the proposed algorithm increases the resilience of the wireless sensor networks.

V. REFERENCES

[1]. V. J. Rathod, M. Mehta, "Security in Wireless Sensor Network:A Survey", Ganpat University Journal of Engineering and Technology, Vol. 1, No. 1, pp. 35-44, 2011.

[2]. H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks", Proceeidngs of IEEE Symposium on Security and Privacy, pp.197, 2003.

[3]. Firdous Kausar, Sajid Hussain, Tai-hoon Kim, and Ashraf Masood, "Attack Resilient Random Key Distribution Scheme for Distributed Sensor Networks", Emerging Direction in Embedded and Ubiquitous Computing Lecture Notes in Computer Science, vol. 4809, pp. 1–11, 2007.

[4]. Jun-Won Ho, "Distributed Detection of Node Capture Attacks in Wireless Sensor Networks", in Smart Wireless Sensor Networks, pp. 345-360, 2010.

[5]. T. Bonaci, L. Bushnell, R. Poovendran, "Node Capture Attacks in Wireless Sensor Networks:A System Theoretic Approach", IEEE Conf. on Decision and Control (CDC), pp. 6765 – 6772, 2010.

[6]. K. Shaila, S. H. Manjula, J. Thriveni, K. R. Venugopal, and L. M. Patnaik, " Resilience Against Node Capture Attack using Asymmetric Matrices in Key Predistribution Scheme in Wireless Sensor Networks", International Journal on Computer Science and Engineering, vol. 3, pp. 3490-3501, 2011.

[7]. Amar Rasheed and Rabi N. Mahapatra, "Key Pre-distribution Schemes for Establishing Pairwise Keys with a Mobile Sink in Sensor Networks", IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 1, pp. 176-184, 2011.

[8]. B. Parno, A. Perrig, and V.D. Gligor, "Distributed Detectionof Node Replication Attacks in Sensor Networks", Proc. IEEE Symp. Security and Privacy (S&P '05), pp. 49-63, 2005.

[9]. Mauro Conti, Roberto Di Pietro,Luigi Vincenzo Mancini, and Alessandro Mei, "Distributed Detection of Clone Attacks in Wireless Sensor Networks", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 5, pp.685-698, 2011.

[10]. M. Zhang, V. Khanapure, S. Chen, and X. Xiao, "Memory efficient protocols for detecting node replication attacks in wireless sensor networks", in proc. 17th IEEE International Conference on Network Protocols (ICNP'09), pp. 284–293,Oct. 2009.

[11]. H. Choi, S. Zhu, and T. Laporta, "SET: Detecting Node Clones in Sensor Networks", International ICST Conference on Security and Privacy in Communication Networks (SecureComm), pp.341-350, September 2007.

[12]. B. Zhu, V.G.K. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient Distributed Detection of Node Replication Attacks in Sensor Networks", Proc. Ann. Computer Security Applications Conf.(ACSAC '07), pp. 257-266, 2007.