Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 13 (12): 2264-2269, 2013
ISSN 1812-5654 / DOI: 10.3923/jas.2013.2264-2269

Research on the Detection Against Replication Attacks in Heterogeneous Wireless Sensor Networks

[1]Xiancun Zhou, [1]Jie Fang, [2,3]Mingxi Li, [4]Yinglai Xu and [4]Yuhui Sun
[1]School of Information Engineering, West Anhui University, Lu'an, 237012, China
[2]School of Computer Science and Technology, University of Science and Technology of China, Hefei, 230026, China
[3]State Key Laboratories of Transducer Technology, Shanghai, 200050, China
[4]New Star Research Institute of Applied Technology, Hefei, 230031, China

Abstract: A number of protocols have been proposed so far to tackle node replication attacks. However, none of these schemes are suitable for wireless sensor networks with mobile nodes. Based on the collaboration mechanism of static and mobile nodes, a multi-point collaboration detection scheme against replication attacks is proposed. The scheme is consist of a polynomial based time-identity related pairwise key predistribution scheme (PTPP) which is used to defend the static network and a challenge/response based collaborative detection scheme (CCD) which is proposed for the detection of mobile replicas. A collaborative detection system is designed on GAINS3 platform. The experiment result shows that the scheme has good performances in embedability and practicality.

Key words: Heterogeneous wireless sensor networks, replication attacks, multi-point collaboration mechanism

INTRODUCTION

Wireless sensor network (WSN) is a self-organizing wireless network composed of sensor nodes deployed in the monitored area. It has been widely used in military and civil field (Akyildiz *et al*., 2002). In security sensitivity application, wireless sensor network is often deployed in the open environment with no custody. Wireless sensor network can be attached by the most destructive means called node replication attack (Parno *et al*., 2005). By capturing sensor nodes, numerous replication nodes similar with the captured nodes are replicated with the reverse analysis technology. Then these nodes are launched into the important regions to wage a variety of attacks of the network. Scholars have put forward detection schemes of node replication attack. Choi *et al*. (2007) divided the network into several disjoint node sets with the communication range of only one jump. A head node is selected in each set to update the node information of the set and regularly report the information to the base station. If there is an intersection among the data of each node set received by the base station, then it can be said that this node is under the node replication attack. Brooks *et al*. (2007) put forward the detection scheme based on key statistics. In the scheme, the base station detects the node replication attack according to the use frequency of the key in the communication between the nodes. The centralized detection scheme above has the problem of single-point of failure. Once the stations or nodes responsible for centralized processing of information are attacked, the entire network defense would be greatly affected. Randomized Multicast (RM) protocol (Parno *et al*., 2005) is the first distributed detection method. This scheme distributes the information of the location of the node to the randomly selected witness nodes. The birthday paradox (Cormen *et al*., 2001) is used to detect replicated nodes. Line-selected Multicast (LSM) (Parno *et al*., 2005) is an improvement of the RM protocol. It reduces the number of witness nodes selected by neighbor nodes, thereby reducing the overhead of the forwarding of the location information and further improving the efficiency of detection. These two agreements have laid a foundation for the detection scheme based on geographical location information. Many later detection schemes of node replication attack of the static network are developed on this basis (Cormen *et al*., 2001; Zhu *et al*., 2007; Ko *et al*., 2009).

In the mobile wireless sensor networks, Yu *et al*. (2008) proposed the XED protocol which utilized the moving and meeting of the nodes. When these nodes encounter with each other, a random number is exchanged. This randomized number is used as the credential of verification when meeting the next time. Ho *et al*. (2009) proposed a centralized detection method.

Corresponding Author: Xiancun Zhou, School of Information Engineering, West Anhui University, Lu'an, Anhui, China

That is, using base station to periodically collect the information about the location of the network nodes. Whether there is a node replication attack is judged through calculating the maximum speed of the nodes and the comparison against the maximum speed of the network. Deng *et al.* (2010) improved the two kinds of protocols above and put forward a detection scheme of distributed node replication attack, that is, the mobility-assisted detection. There exists a possibility of mutual collusion and conspiracy to avoid the detection of the node replication attack. Xing and Cheng (2010) put forward a detection scheme of the validity of the time and the location of the node replication. The scheme is divided into Time Domain Detection scheme (TDD) and the Space Domain Detection (SDD).

With the wide application of wireless sensor network in various fields, heterogeneous networks consisting of static networks and mobile networks have appeared. This brings greater challenges to the detection of node replication attack. Therefore, enhancing the adaptiveness of the detection scheme of node replication to the network structure has become a hot topic. Targeted at the heterogeneous wireless sensor networks consisting of static nodes and mobile nodes, this study proposes a new detection scheme of node replication attack.

DETECTION SCHEME

Network model and assumptions: Assume that the heterogeneous network is composed of static nodes, mobile nodes and access point. For the convenience of describing the detection scheme, the following assumptions of the network could be made: (1) Static sensor nodes are uniformly distributed in the monitored region D. In this study, it is assumed that the network uses Low Energy Adaptive Clustering Hierarchy (LEACH) algorithm. (2) The mobile network has the same monitored area as the static network. The mobile node moves according to the rule of the specific mobile model such as the random direction model.

Detection scheme of node replication attack based on multi-point collaboration: Collaborative detection scheme is composed Polynomial-based Time-identity related Pairwise key Predistribution scheme (PTPP) and Challenge/response-based Collaborative Detection scheme (CCD). The PTPP scheme is the solution scheme of the static network. It takes advantage of the characteristics of uniqueness of time and ID of the node deployment to enforce defense against the node replication attack. A quaternary symmetric polynomial of times is used to bind the node deployment time with ID. On this basis, the negotiation mechanism of shared pairwise key between nodes is established. Thus, the replicated nodes could neither forge a new node ID, nor join the network outside the region of the captured nodes by modifying the deployment time. CCD scheme is mainly used in mobile network. It stores the trajectories of mobile node in the static network. Through the collaborative detection of static networks and mobile networks, the replicated nodes in the mobile network are detected. PTPP scheme is used in the CCD scheme. If a mobile node reaches the monitoring scope of a cluster in the network, the cluster head node would request the node to leave a random number as the credentials of arrival. If multiple replicated nodes all reach the same cluster, then these nodes would be detected.

PTPP scheme: Before deployment, a quaternary symmetric polynomial with t (such as Eq. 1) is loaded at each node:

$$P(x,y,u,v) = \sum_{i,j,k,l=0}^{t} a_{ijkl} x^i y^j u^k v^l \left(a_{ijkl} \in F_q\right) \qquad (1)$$

where, F_q is the finite field and q is a large prime number.

Symmetry means that for any permutation of x, y, u and v, the values of the polynomial are all equal. For example:

$$P(x, y, u, v) = P(u, y, x, v)$$

After each node is deployed, the deployment time t_u of their own should be obtained; then the t_u and node ID ID_u are substituted into Eq. 1 to generate a binary polynomial $F_u(x, y) = P(t_u, ID_u, x, y)$. Then the original polynomial P(x, y, u, v) is permanently deleted.

Node u is taken as an example. When the initialization is completed, it would broadcast the key establishment request message (KERM) to the neighbor node, with the format of the packet as $<ID_u, t_u>$. Considering the unreliability of wireless links, node u with higher probability. m is the system parameters. The last broadcast time b_u is recorded. If some peripheral node still have not received the data package after m times of KERM broadcast, then these node could not become the neighbor nodes of node u. In large-scale wireless sensor networks, however, the lack of individual neighbor is a normal phenomenon which would not affect the operation of the network.

The neighbors of node u start to establish a shared pairwise key after receiving the KERM broadcasts. This involves two processes. One is the processing of KERM

data package and the other is the processing of Key Establishment Response Message (KEREM).

The processing of KERM data package is described as follows: After the neighbor node u receives its KERM data package, it would first determine whether the difference between the node deployment time u is less than T_{min}. If not, this means that the node u has missed the time to establish shared pairwise key with node w. Then the node w would refuse to establish key with node u. If yes, then node w would substitute the received ID_u and t_u into their own binary polynomial, to calculate the pairwise key u. Whether the node b_w and t_u. If $b_w = t_u$, then node u is deployed after they broadcast KERM. Thus it is unable to receive their own KERM. Then the KEREM is replied to the node u in the format of $<ID_w, t_w>$. Otherwise, node u is deployed before they broadcast KERM. Thus it could receive their own KERM. Then the KEREM is not replied to the node u.

The processing of KEREM data package is described as follows: After node u receives the KEREM of node w, then ID_w and t_w are obtained and are substituted into their own polynomial to obtain $K_{uw} = F_u (ID_w, t_w)$. If node u is a replicated node, the deployment time or ID is modified to avoid detection. There must be $K_{uw} \leq k_{wu}$. Then it would not be able to establish shared pairwise keys with its neighbor nodes. If the node u is the valid node, node w is deployed before node u. Therefore it also needs to be verified with other neighbor nodes. Then node u would broadcast the information of the detection node w. The forwarding time is set as 1. After the neighbor node of node u receives this message, it is checked whether the node is present in the neighbor list. If the node exists, then it would stop forwarding and try to encrypt the communication to ensure that the communication link is smooth. If yes, the information that the node has passed the detection is replied to node u. If there is no intersection, then the message is forwarded to the neighbor nodes of the list and the forwarding time is set as 0. That is to say, the node that receives the message would not forward the message, regardless whether there is a node w in its neighbor list. If the node is in the neighbor list, then the encrypted communication with it is tried to confirm whether the communication link is smooth. The information of passed or failed detection is sent back to the node u through the nodes which forward the message. If node u sent by other nodes, then the corresponding node would be listed as its neighbor node. Thus, the shared pairwise key is built. Otherwise the generated key would be deleted.

Challenge/response based collaborative detection scheme (CCD): After deployed in the monitored area, the mobile nodes move freely. At this time, the static network has formed a cluster structure according to LEACH protocol, the shared pairwise keys among neighbor nodes are established. Assume the static nodes detect the mobile node v. If it is not a cluster head node, then the detected mobile node is reported to its cluster head. After the cluster head node u receives the report of cluster member nodes (or detects the mobile node), then it will negotiate with it on the shared pairwise key in accordance with the PTPP protocol to prevent the attack on node and the forgery of ID. Then the cue of entering into the cluster is sent to node v, in the format of $\langle k_{vu} (C_i)\rangle$. Where C_i is the number of cluster. The current time t^v_{arrive} and the time set for waiting for response t_r are recorded. After the mobile node v receives the cue, it would reply the arrival time t^i_{arrive} and the cluster generated random number r_i (password) to node u, in the format as $\langle K_{vu}(t^i_{arrive}, r_i)\rangle$. C_i, the time of arrival and the password are recorded in their memory table, as shown in Table 1. After node u receives the reply, it compares t^i_{arrive} with the recorded t^v_{arrive}. If it is in the allowable range of error of time synchronization, t^i_{arrive} is saved as t^v_{arrive} and r_i is saved as r_v, otherwise node v would be considered as the replicated node.

Then this node is located and the result of its location is sent back to the nearest AP.

In order to avoid the loss of password records due to the capture of cluster head node, the cluster head node u randomly selects n_c nodes in the cluster member nodes. Then the ID, the arrival time v are sent to them, in the format of $K_{ui} (ID_v, t^v_{arrive}, r_v)$. j is the selected node. In the meantime, the memory table is established, as shown in Table 2. After the cluster member nodes of cluster C_i receives the data, these nodes would store these data into its own memory table, as shown in Table 3. Therefore, even if the records are lost, these node could also query each other to re-establish the memory table.

When node v once again arrives at the monitored area of cluster C_i and is detected by any cluster member node, then node u would establish the encrypted communication links in accordance with the PTPP

Table 1: Storage table of mobile nodes

Cluster No.	C_1	C_4	C_{10}	.....
Time and password	$\langle t^1_{arrive}, r_1\rangle$	$\langle t^4_{arrive}, r_4\rangle$	$\langle t^{10}_{arrive}, r_{10}\rangle$	.....

Table 2: Storage table in the cluster head nodes

Members of the cluster	u_1	u_2	u_3	.....
Password index of mobile nodes	v_1	v_1	NA	.....
	v_2	NA	v_2	.....
	.....	.....	.....	.....

Table 3: Storage table in members of the cluster

Mobile nodes	v_1	v_5	v_6	.....
Time and password	(t^1_{arrive}, r_1)	(T^5_{arrive}, r_5)	(T^6_{arrive}, r_6)	.....

protocol after negotiating with it on the shared pairwise key. Then the cue of entering into the cluster is sent to the node. The time waiting for reply is set as t_r. If the time taken is longer than that, then the same operation above should be executed. After the mobile node v receives the cue, it would find the time and the password information left when the nodes arrive at the cluster the last time from their own memory table. At the same time, a new password is generated. These are all sent to node u. After receiving the message, node u would find the cluster member nodes that store the information of node u according to the ID from the memory table. Then the message is forwarded to them. The cluster member nodes which receive the message would check t^v_{arrive} and r_v simultaneously. If they are correct, it would report to the cluster head node that the detection has passed. Otherwise, it would report that the detection has failed. If the detection is passed, node u would store the new password according to the above operation, then a successfully updated message is replied to node u. After receiving the message, node v would also update the password and time of arrival of cluster C_i. On the contrary, if the detection fails, then it is considered that the node is under the node replication attack. Then its ID is reported to AP.

EXPERIMENTAL ANALYSIS

GAINS3 wireless sensor network development platform by Integrated Circuit Design Center of the Chinese Academy of Sciences in Ningbo is used. The sensor module is made of optical temperature sensor. The processor and memory are made of the ATmega128L chip and the AT45DB chip, respectively. The transceiver is made of the radio-frequency chip CC1000. The system is composed of a wireless sensor network and data processing terminal. The wireless sensor network consists of mobile nodes and static nodes. Besides specific monitoring tasks, it could accomplish the real-time detection and defense against node replication attack. The data terminal is responsible for centralized processing of the monitoring data and the detection data sent back to the network, sending control command to the network and displaying the results of data processing. The experiment uses 33 GAINS3 sensor nodes (including 20 static nodes, 10 mobile nodes, 1 AP node and 2 interfering nodes). The 20 static nodes are randomly distributed in a square monitored region with an area of 10×20 m. These nodes are self-organized into a small static network. The 10 mobile nodes move randomly in the monitored area according to the Random Waypoint model, with the moving speed of 0.5~1.5 m sec^{-1} and the residence time of

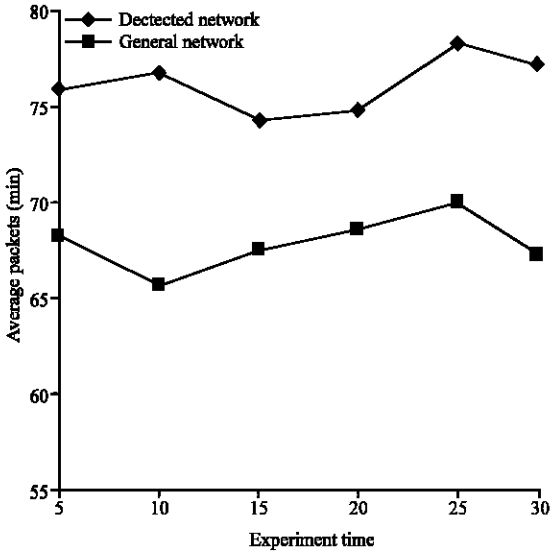

Fig. 1: Energy consumption comparison

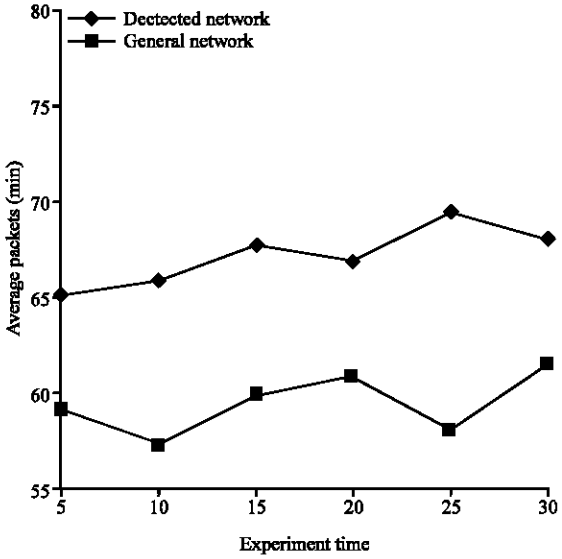

Fig. 2: Service quality comparison

0~5 sec. Two interfering node are placed at both ends of the diagonal of the monitored area.

First, the verification experiment of the embedability of the detection scheme is analyzed. As shown in Fig. 1 and 2, when the collaborative detection scheme is not introduced, the average number of data packages sent per minute and that of the monitoring data packages sent per minute of the network are basically the same. The numbers are 67.6 in Fig. 1 and 68.2 in Fig. 2, respectively. The purpose of sending the data package is solely the transmission of the monitoring data. Larger fluctuation at each time interval is caused by the communication

Fig. 3: Evading attack comparison chart

interference of the interfering node and the failure of part of the network nodes. After the collaborative detection scheme is introduced, the average number of package sent per minute of the network increases to 76.5, as shown in Fig. 1. The number of monitoring packages sent decreases to 59.7, as shown in Fig. 2. At this time, due to the execution of the detection scheme, the total communication amount of the network increases slightly. The data package sent is divided into two categories. One category is used for the transmission of detection data and the other is used for the transmission of monitoring data, which causes the service quality of the network to decline. As most energy consumption of sensor nodes is in the wireless communication module, the total communication amount could be used for the comparison of energy consumption. It could be seen from the experimental results that the newly added detection scheme increases the energy consumption of the network by 12.3%, while the service quality has fallen by 13.6%. Therefore, this scheme has good embedability.

Secondly, the detection experiment of the protocol is analyzed. In Fig. 3, when the replicated nodes do not adopt the elusion strategy to avoid detection, the detection time would become shorter with the increase of the replicated nodes n. It is reduced to 0.3 sec at n = 5. When the replicated nodes selectively leave the password to avoid detection in the process of movement, the detection time is slightly larger than that under the same conditions without the elusion of attack. This is because the network appropriately relaxes the condition of mandatory detection in order to avoid false alarm of the detection scheme.

CONCLUSION

In this study, the node replication attack and the corresponding detection scheme in wireless sensor network (WSN) are studied based on the characteristics of the application of wireless sensor network. Targeted at the heterogeneous networks consisting of static networks and mobile networks, the collaborative detection scheme and the defense of node replication attack based on the collaboration of the static network and the mobile network is proposed. The collaborative detection system is designed. The verification experiment shows that the scheme is secure and effective. It is a very practical detection scheme.

ACKNOWLEDGMENT

This study was supported by the National Natural Science Foundation of China under Grant No. 61303209 and 61302179, the Nature Science Foundation of Anhui Education Department under Grant No. KJ2013A255, the Science Foundation of State Key Laboratories of Transducer Technology under Grant No. SKT1206 and the Directional Entrusting Research Projects of Lu'an under Grant No. 2012LWA015.

REFERENCES

Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. A survey on sensor networks. IEEE Commun. Mag., 40: 102-114.

Brooks, R.R., P.Y. Govindaraju, M. Pirretti, N. Vijaykrishnan and M.T. Kandemir, 2007. On the detection of clones in sensor networks using random key predistribution. IEEE Trans. Syst. Man Cybernet. Part C: Appl. Rev., 37: 1246-1258.

Choi, H., S. Zhu and T.F. La Porta, 2007. SET: Detecting node clones in sensor networks. Proceedings of the 3rd International Conference on Security and Privacy in Communications Networks and the Workshops, September 17-21, 2007, Nice, France, pp: 341-350.

Cormen, T.H., C.E. Leiserson, R.L. Rivest and C. Stein, 2001. Introduction to Algorithms. 2nd Edn., The MIT Press, Cambridge, UK., ISBN-13: 9780262032933, Pages: 1180.

Deng, X.M., Y. Xiong and D.P. Chen, 2010. Mobility-assisted detection of the replication attacks in mobile wireless sensor networks. Proceedings of the IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications, October 11-13, 2010, Niagara Falls, Canada, pp: 225-232.

Ho, J.W., M. Wright and S. Das, 2009. Fast detection of replica node attacks in mobile sensor networks using sequential analysis. Proceedings of the 28th IEEE International Conference on Computer Communications, April 19-25 2009, Rio de Janeiro, Brazil, pp: 1773-1781.

Ko, L.C., H.Y. Chen and G.R. Lin, 2009. A neighbor-based detection scheme for wireless sensor networks against node replication attacks. Proceedings of the International Conference on Ultra Modern Telecommunications and Workshops, October 12-14, 2009, St. Petersburg, Russia, pp: 1-6.

Parno, B., A. Perrig and V. Gligor, 2005. Distributed detection of node replication attacks in sensor networks. Proceedings of the IEEE Symposium on Security and Privacy, May 8-11, 2005, Oakland, CA., USA., pp: 49-63.

Xing, K. and X.Z. Cheng, 2010. From time domain to space domain: Detecting replica attacks in mobile ad hoc networks. Proceedings of the 29th IEEE International Conference on Computer Communications, March 14-19, 2010, San Diego, CA., USA., pp: 1-9.

Yu, C.M., C.S. Lu and S.Y. Kuo, 2008. Mobile sensor network resilient against node replication attacks. Proceedings of the 5th Annual IEEE Communications Society Conference on Sensor, Mesh and *ad hoc* Communications and Networks, June 16-20, 2008, San Francisco, CA., USA., pp: 597-599.

Zhu, B., V.G.K. Addada, S. Setia, S. Jajodia and S. Roy, 2007. Efficient distributed detection of node replication attacks in sensor networks. Proceedings of the 23rd Annual Computer Security Applications Conference, December 10-14, 2007, Miami Beach, FL., USA., pp: 257-267.