DRMWSN-Detecting Replica Nodes Using Multiple Identities in Wireless Sensor Network

Nagaraj Ambika and G.T. Raju

Dayananda Sagar College of Engineering,
Research Scholar of Bharathiar University, Bangalore, India
Prof & Head, Dept of CS & Engg, RNSIT, Bangalore
ambika.nagaraj76@gmail.com, drgtraju_rnsit@yahoo.com

Abstract. Wireless sensor network are prone to different types of attacks due to lack of supervision. Trusting the data received from the network becomes quite difficult. Implementing prevention and detection techniques provide strong impediment to the network from getting compromised. In this paper both the techniques are being utilized providing better reliance over the data being communicated. Pair-wise keys and group wise keys are being generated, which also provides identity of the nodes at that instant of time. This technique deters wormhole attack to a large extent.

Keywords: prevention and detection technique, steganography, group-key generation, pair-wise key generation.

1 Introduction

Wireless sensor network are low cost nodes deployed in unattended areas which sense, collect and transmit data to the base station. These nodes are used widely in many applications like habitat monitoring [1], [2] [3], forest fire detection [4], [5], military applications [6] and so on. These nodes are prone to failures due to the low manufacturing cost. These nodes are limited in power and hence the battery power needs to be utilized carefully. This pursues them to change the topology frequently. As these nodes are utilized to send some classified material, the chances of these nodes getting hacked are quite discernible. An adversary can take control of the nodes or can modify the information sent in the course of its travel. The adversaries can pose itself as one of the nodes and try to gather all the data sent by other nodes. To counteract this type of attacks, data is encrypted accompanied by authenticating the nodes. To bring this act in to play, the nodes can either prevent itself getting compromised or the base station/ neighboring node/ cluster head can detect the compromised node and can cease to send data to the compromised node. Using both the techniques together would help to elevate the security of the network by guarding the data from unauthorized acsessors.

Many preventive and detection algorithms [17] are being suggested. This paper is based on graph theory. Pair-wise key is generated using bipartite graph. Group keys are generated using multipartite graph and Hungarian algorithm. The paper also

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 866–878, 2013.

utilizes steganography, a technique used to transmit message hidden inside another text message. Steganography [9] is a technique through which the data which is communicated does not come to the notice of its adversaries.

This paper is being divided into sections. Section 1&2 gives a description of the graph theory and set theory concepts utilized in the paper. Section 3 provides related work done in the similar field. Section 4 provides a detail description of proposed model. Section 5 furnishes the simulated results of how the suggested protocol escalates security in the network. Section 6 provides the conclusion and suggests the further work in this field.

2 Preliminaries and Notations

Consider the entire network as a subset of clusters. The cluster is represented as a sub-graph and the union of all the sub-graph constitutes the network. Each node in the cluster is considered as a vertex and the keys generated are considered as edges.

The nodes are pre-deployed with keys which are mutually exclusive from each other. The nodes can generate pair-wise key or a group key. Two nodes from the cluster are chosen to generate pair-wise key.

Table 1. Notations used in DRMWSN

Notation	Meaning
D	Detector
BS	Base station/ sink
$N_i \rightarrow N$	Ni node in the cluster broadcast HELLO message
C_i	ith Cluster in the network
A→ B:msg	A sends message to B
BS → N : msg	Base station broadcast message to the network N
$K \rightarrow K_i \| K_i$	Generation pair-wise key
$K \rightarrow K_i \| K_i \| K_m \| K_n \| K_o$	Generation of group key
$K(N_i)$	Key of node N_i
G	Entire network considered as graph
S	Steganography message broadcasted by the base Station
ADDR(OFFSET_ADDR)	OFFSET_ADDR considered as the starting address
ADDR(STEGO_MSG)	Address dispatched by the base station using steganography
EN_DATA(N_i)	Encrypted data of node N_i

Definition 1: let B be a bipartite graph if there is $N_1,N_2...N_n \subseteq G_i$ where I = {1,2.……n}. let N_i ={K_1, K_2,…….K_n }be the set of keys stored in the node such that K(Ni) ∩ K(Nj) = ∞ .

Definition 2: let B be a multipartite graph if there is N1,N2...Nn ⊆ Gi where I = {1,2.……n}. let Ni ={K_1, K_2,…….K_n }be the set of keys stored in the node such that $K(N_i) \cap K(N_j) \cap$ ……..$K(N_m)$ =∞.

Definition 3: Consider the bipartite graph B, let F: $K(N_i) \rightarrow K(N_j)$ be a mapping between the unmatched keys of the nodes.

Definition 4: let S= $S_1 \cup S_2 \cup$….. ∪ S_n be the message broadcasted by the base station to the network . Calculate (F: $K(N_i) \rightarrow K(N_j)$) → ((ADDR($K(N_i)$) ∪ offset_addr) ⊆ S)

3 Related Work

In [23] a framework is provided which is used to study the security of key pre-distribution schemes. During the key pre-distribution phase, key information is assigned to each node, such that after deployment, neighboring sensor nodes can find a secret key between them. key pre-distribution phase generates G and D matrices, followed by the selection of a key space. Then, in the key agreement phase, after deployment, each node discovers whether it shares any key space with its neighbors. To achieve this, each node broadcasts a message containing the node's ID, the indices of key spaces it carries, and the seed of the column of G it carries. The paper proposes a new key pre-distribution scheme which substantially improves the resilience of the network compared to previous schemes, and give an in-depth analysis of our scheme in terms of network resilience and associated overhead.

In [19] Erdos and Renyi component theory is utilized. This theory shows inspite of small node's degree the network remains connected. The paper evaluates relation between connectivity, memory size and security.

In [17] authentication-based intrusion prevention and energy-saved intrusion prevention is being utilized to improve security of cluster-based sensor network. The member nodes take turn to monitor the cluster head.

[20] presents a deterministic key distribution scheme based on Expander Graphs. It shows how to map the parameters (e.g., degree, expansion, and diameter) of a Ramanujan Expander Graph to the desired properties of a key distribution scheme for a physical network topology.

4 Intruder Model

The intruder's main intention is to take control of the entire network. It can accomplish this task by taking control of all the nodes in the network. The intruder with the help of a compromising node can mask itself as one among them and divert all the traffic towards itself, thereby draining the energy of the network and can

mislead the base station by modifying the data being sent by other nodes of the network. Other uncompromised nodes in the network will be unable to find the intention of the intruder and will hence share some secret information within them. If other nodes utilize the same encryption key distributed by the compromise node, the intruder after blocking the data can decrypt data easily. This activity not only affect the cluster in which the compromised node reside, but also the other nodes in the network as the compromised node can advertise itself as a node near to the base station. Uncompromised nodes in-turn divert all their data to this compromised node. The intruder can make a replica of the compromised nodes and place them in different location and can take the control of the entire network.

5 DRMWSN Model

5.1 System Model

The paper utilizes Tinynode 584 to be distributed in the required environment. It is a low powered OEM module providing simple and reliable way to add wireless communication to sensors. TinyNode 584 is optimized to run TinyOS and packaged as a complete wireless subsystem with 19 configurable I/O pins offering up to 6 analog inputs, up to 2 analog outputs.

Table 2. illustrates the current consumption of TinyNode

Mode	Energy Consumption
Sleep, time off	0.004 mA
Sleep, time on	0.007 mA
μC only	2 mA
Receive	16 mA
Transmit(0dbm)	25 mA
Transmit(10dbm)	46 mA

5.2 Key Distribution and Deployment of Sensors in the Field

Set of keys are generated by the base station. All the sensors are embedded with subset of keys. Care is taken that the keys are mutually exclusive. Each node has an offset address(signifies the actual starting address i.e. the node masks over the actual address to calculate the starting address) , which differs from the rest of the other cluster members.

5.3 Formation of Cluster

To authenticate each other, unique id's are embedded inside sensors. The sensors after deployment broadcast HELLO message. The sensors which respond to the broadcasted message are pooled to form a cluster. They authenticate each other by

utilizing encrypted unique ID stored inside them. After the cluster is formed, the cluster members choose the cluster head and the subsequent node depending on the energy stored in each node.

$$N_i \rightarrow N{:}msg$$

5.4 Communications between Cluster Members and Base Station

Steganography is an art and science used to embed secret data inside the cover data by utilizing embedded algorithm and steganography key. This paper utilizes this technique, where the base station broadcast message to the entire network by embedding the key inside the cover text.

$$BS \rightarrow N : msg$$

5.5 Generating of Key

5.5.1 Generation of Pair-Wise Key

The nodes in the network have to interpret the message sent by the base station. The nodes have to obtain the location of key , identify which node should participate in generation of the key,& global time. Within the time limit the key has to be generated and distributed to other members of the cluster. The nodes authenticate each other and form a pair-wise key.

$$START\_ADDR \rightarrow OFFSET\_ADDR$$

$$K_i \rightarrow ADDR(STEGO\_MSG)$$

$$K \rightarrow K_i \| K_j$$

$$K \rightarrow C_i$$

Every node differs in their offset address. The offset address is added to the location obtained from the steganography message broadcasted by the base station. Hence the mapping between the keys is decided by the base station. The base station will have a prior idea as to which key is being utilized in the pair-wise key[18] generation. If any nodes do not respond within the time limit, the detector isolates the node and keeps the node under observation. If Ith node respond with Ki key within the time limit and jth node does not respond , then Ki is declared as the key to encrypt the messages. considering $K_j = \infty$

$$K \rightarrow K_i \ \phi$$

After several observations, the suspected node if termed as compromised node, its ID is removed and the detector D sends a message to the base station, which in turn broadcast the message to the network

$$D \rightarrow BS{:}msg$$

$$BS \rightarrow N{:}msg$$

The generated key is being distributed to the cluster members and the members of the cluster in turn encrypt the data to be transmitted using the key. The message is forwarded to the next cluster head by the present cluster head.

$$N_C \rightarrow EN\_DATA(N_i) \| EN\_DATA(N_j) \| EN\_DATA(N_j) \| EN\_DATA(N_m) \| EN\_DATA(N_n) \| EN\_DATA(N_o)$$

5.5.2 Generating Group-Key

All the nodes in the cluster participate forming a group key utilized to encrypt the sensed data. After receiving the broadcasted message from the base station, all the nodes should start to form a group key. If the key from any one of the nodes is not transmitted during the time limit, the node comes under suspicion that it may be a compromised node. After some amount of observations the suspected node is confirmed to be compromised or uncompromised node. If the detector D concludes the suspected node to be compromised node as a compromised node, the detector sends the report to the base station. The base station in turn broadcast the message to the network.

$$START\_ADDR \rightarrow OFFSET\_ADDR$$

$$K_i \rightarrow ADDR(STEGO\_MSG)$$

$$K \rightarrow K_i \| K_j \| K_m \| K_n \| K_o$$

$$K \rightarrow C_i$$

$$D \rightarrow BS{:}msg$$

$$BS \rightarrow N{:}msg$$

If one of the key is not been in the participation, then that key is assumed to be null and the rest of thenodes participate to generated the group key. The key is been distributed to the rest of the cluster members to encrypt the data.

$$K \rightarrow K_i \| K_j \| K_m \| k_n \| K_o$$

$$N_C \rightarrow EN\_DATA(N_i) \| EN\_DATA(N_j) \| EN\_DATA(N_j) \| EN\_DATA(N_m) \| EN\_DATA(N_n) \| EN\_DATA(N_o)$$

6 Security Analysis

The following scenario is considered.

6.1 Cluster Head/Subsequent Node Is Compromised

Subsequent node and the cluster head authenticate each other, hence if any one of the node is compromised the report is generated by the other and sent to the base station. The base station broadcast the blacklisted node to other nodes in the network. The cluster which has the compromised node, chooses another node in its place. If both the cluster head and subsequent nodes are compromised, the node will not be able to read the hidden message broadcasted by the base station. Either the node will not transmit the packets in the scheduled time or will utilize different keys for encryption. If the base station suspects that the cluster head and subsequent node are compromised, it informs other nodes in the network to black list them. Other nodes in the cluster elect their cluster head and subsequent nodes among themselves.

6.2 Cluster Members Are Compromised

If any of the cluster members are compromised, the cluster head will know at the time of authentication. The cluster head sends the report to the base station. The base station in turn, broadcasts the message to other nodes in the network. The nodes in the network mark this node as blacklisted node and do not accept or forwards packets to this node.

7 Simulated Results

The work is simulated using NS2. Considering the length of the encryption key to be 128 bits, tiny node can store around 512 keys. Hence a cluster can generate 512 combination of keys. The following are the outcomes of the paper.

Table 3. Simulated Results

	Pair-wise keys	Group keys
Distribution of nodes	Uniform	Uniform
Number of nodes in the network	Multiples of 1000	Multiples of 1000
Probability of detection of compromised nodes	>=0.4	>=0.99
Probability of false alarm	<=0.1	<=0.001
Probability of data integrity	>=0.8	>=0.98
Probability of reliable data reaching base station	>=0.89	>=0.98

7.1 Energy Consumption

Energy is one of the important features in wireless sensor network. As the sensors are deployed in unattended areas, the battery cannot be recharged. Sensors either run out

of battery power or come under the control of the adversaries. In both the cases, the network will get shortage of sensors which in turn will not provide accurate readings. Hence to avoid the loss, the battery power has to be consumed very carefully. but at the same time a prevention mechanism has to be implemented so that the sensors are provided with a protective shield to safe guard themselves. This paper provides detection and prevention model which better protection against the adversaries. This paper utilizes 24% more energy than a normal pre- distribution key use in wireless sensor network (PKWSN). Utilizing this technique helps the sensors to shield itself from the adversaries and in any case if any sensor gets compromised, the rest of the nodes in the cluster is prevented from getting compromised.

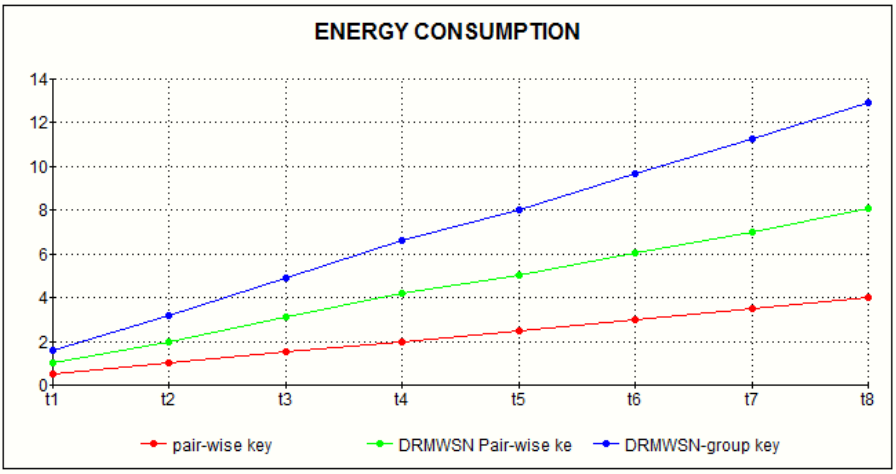

Fig. 1. Energy Consumption in PKWSN and DRMWSN

7.2 Sybil Attack

One of the priority security issues in any kind of network would be authentication. Unless the receiver is an authorized node to receive the data, there is a large possibility that the data can get modified leading to breach integrity. In a large network consisting of multiples of thousands of nodes, it is quite a difficult task to keep a track of data being transferred from one node to another. Hence every cluster have to shield itself from such types of attack. The primary task to avert such type of attacks is to device a strong authentication technique which makes it unique from other clusters. The base station will find it intricate if each node has a unique authentication code. The process simplifies if each cluster has an authentication code which cannot be replicated by adversary. This paper utilizes a technique where in any two nodes of the cluster involving in generating pair-wise key will make the network

secure. This also provides authentication of the source (cluster). If the mapping goes wrong in any one of the cluster, the base station will be able to track it easily and consider it as malicious node by evaluating the report sent by the detector of the cluster. This paper provides 22.3% more security than a regular pre-distribution key in network (PKWSN). The fig 2, provides a pictorial representation of PKWSN and DRMWSN against Sybil attack [14], [15], [16]. X-axis denotes the time and Y-axis denotes percentage of nodes deployed.

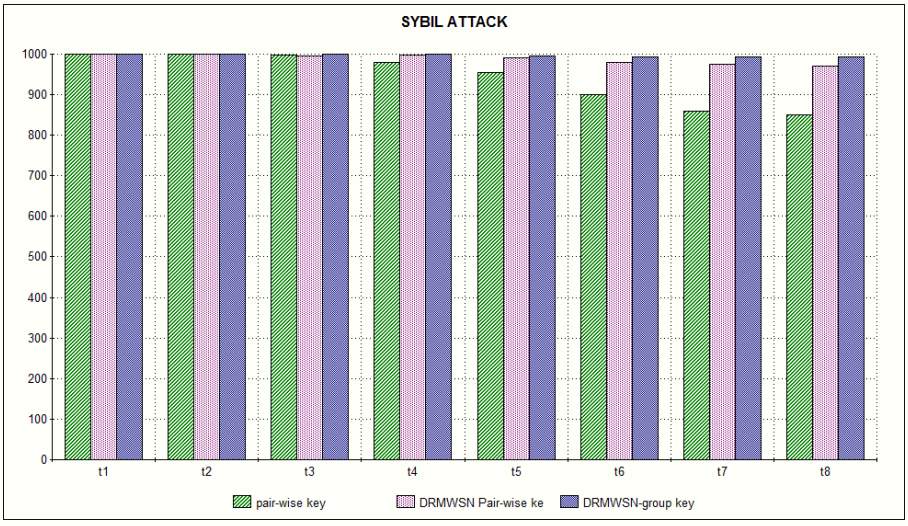

Fig. 2. Illustration of Sybil attack in PKWSN and DRMWSN

7.3 Sinkhole Attack

Sinkhole attack[11], [12], [13], [24],[26] is a type of attack, which attracts all the traffic towards itself posing as one of the vested nodes in the network to which nodes could forward the data. It disguises itself as the one of the nodes nearer to the base station. If the node is positioned nearer to the base station, it acquires almost all the packets moving towards the base station. The adversary can modify the packets or can even deny forwarding the packets towards the base station. This paper reduces this attack by 8.4%. Fig 3 illustrates the working of DRMWSN against sinkhole attack and provides a comparison to PKWSN. The nodes in the network will change the encryption key when ever intimated by the base station which keeps the data safe from the adversary. The nodes will be on continuous check by detector. As the cluster members are authenticated continuously after every session, the compromised nodes can be detected and notified.

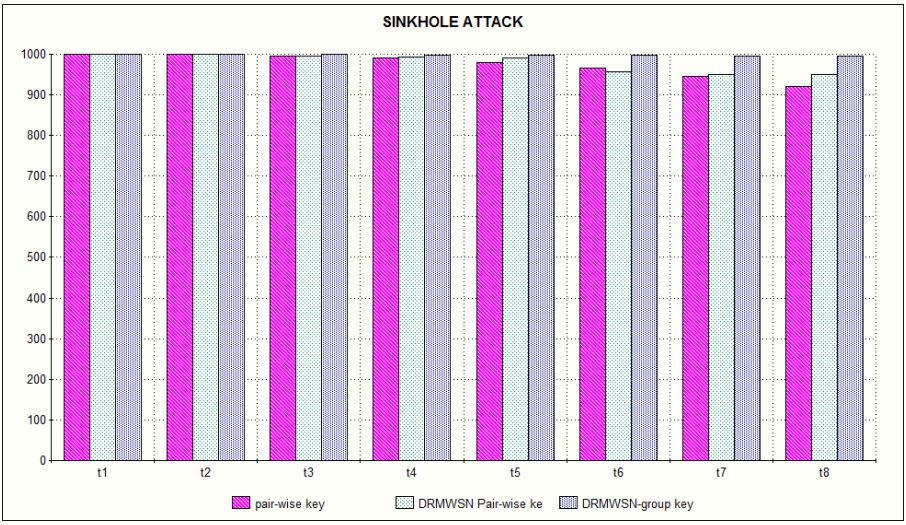

Fig. 3. Illustration of Sinkhole attack in PKWSN and DRMWSN

7.4 Wormhole Attack

Wormhole attack [7], [8], [25], [9], [10] is a kind of attack where the adversary tunnels the data from one location to another and retransmits the data. Due to this activity the base station will not get correct readings from the exact location. Added to this, the base station will not receive the required information in time. This paper secures the network by 16.3% against wormhole attack. The base station will have a prior knowledge of the keys being stored in each sensor node and as the keys keep on changing the base station will be able to detect the compromised node in the network.

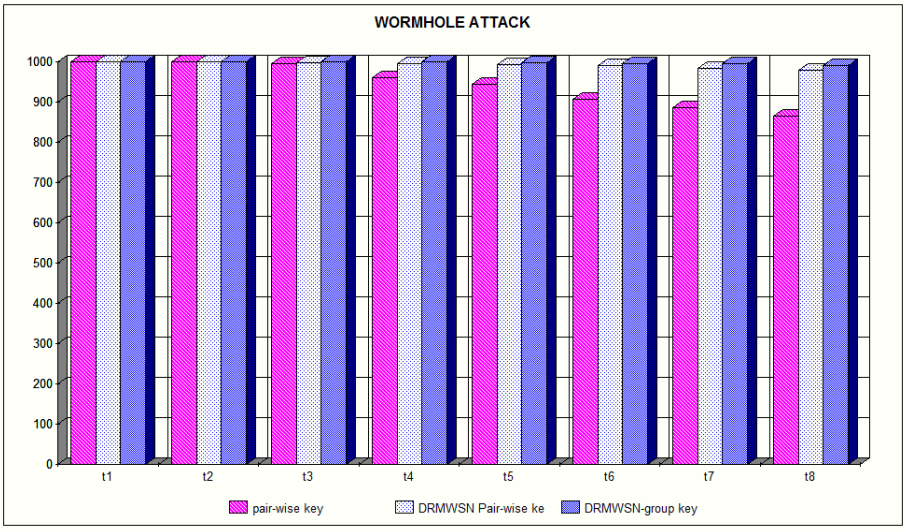

Fig. 4. Illustration of Wormhole attack in PKWSN and DRMWSN

Fig. 5. Implementation of DRMWSN on nodes

8 Conclusion

This paper increases the security of the network to a larger extent. The paper is based on graph theory and set theory. The pair-wise key/group key is established by the nodes of the cluster and being circulated to other members of the cluster. The keys are unique among themselves and changing of the encryption keys after every broadcast by the base station makes it more resilient against different kinds of attack. The base station utilizes steganography technique to transmit data which it needs to communicate to its nodes in the network. This in turn makes the transmission safer.

References

1. Mainwaring, A., Culler, D., Polastre, J., Polastre, J., Polastre, J.: Wireless Sensor Networks For Habitat Monitoring. In: Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications, doi:10.1145/570738.570751
2. Szewczyk, R., Osterweil, E., Polastre, J., Hamilton, M., Hamilton, M., Hamilton, M.: Habitat monitoring with sensor networks. Magazine of Communications of the ACM - Wireless Sensor Networks 47(6) (2004)
3. Naumowicz, T., Freeman, R., Kirk, H., Dean, B., Calsyn, M., Liers, A., Braendle, A., Guilford, T., Schiller, J.: Wireless Sensor Network for habitat monitoring on Skomer Island. In: IEEE 35th Conference on Local Computer Networks (LCN), pp. 882–889 (2010), doi:10.1109/LCN.2010.5735827
4. Hefeeda, M., Bagheri, M.: Wireless Sensor Networks for Early Detection of Forest Fires. In: IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems, pp. 1–6. Simon Fraser Univ., Surrey (2007), doi:10.1109/MOBHOC.2007.4428702
5. Mal-Sarkar, S., Sikder, I.U., Konangi, V.K.: Application of wireless sensor networks in forest fire detection under uncertainty. In: 13th International Conference on Computer and Information Technology (ICCIT), pp. 193–197 (2010), 10.1109/ICCITECHN.2010. 5723853

6. Lee, S.H., Lee, S., Song, H., Lee, H.S.: Wireless sensor network design for tactical military applications: Remote largescale environments. In: Military Communications Conference, pp. 1–7. IEEE (2009), doi:10.1109/MILCOM.2009.5379900
7. Hu, Y.-C., Perrig, A., Johnson, D.B.: Wormhole attacks in wireless networks. IEEE Journal on Selected Areas in Commnication 24(2), 370–380 (2005)
8. Zhao, Z., Wei, B., Dong, X., Yao, L., Gao, F.: Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis. In: International Conference on Information Engineering (ICIE), pp. 251–254 (2010), doi:10.1109/ICIE.2010.66
9. Chen, H., Lou, W., Sun, X., Wang, Z.: A secure localization approach against wormhole attacks using distance consistency. Journal EURASIP Journal on Wireless Communications and Networking - Special Issue on Wireless Network Algorithms, Systems, and Applications 2010, doi:10.1155/2010/627039
10. Modirkhazeni, A., Aghamahmoodi, S., Modirkhazeni, A., Niknejad, N.: In: The 7th International Conference on Networked Computing (INC), pp. 122–128 (2011)
11. Sharmila, S., Umamaheswari, G.: Detection of Sinkhole Attack in Wireless Sensor Networks Using Message Digest Algorithms. In: International Conference on Process Automation, Control and Computing (PACC), pp. 1–6 (2011), doi:10.1109/PACC. 2011.5978973
12. Krontiris, I., Giannetsos, T., Dimitriou, T.: Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side. In: IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, WIMOB 2008, pp. 526–531 (2008), doi:10.1109/WiMob.2008.83
13. Ngai, E.C.H., Liu, J., Lyu, M.R.: An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. Journal Computer Communications 30(11-12) (2007), doi:10.1016/j.comcom.2007.04.025
14. Ssu, K.-F., Wang, W.-T., Chang, W.-C.: Detecting Sybil attacks in Wireless Sensor Networks using neighboring information. The International Journal of Computer and Telecommunications Networking 53(18) (2009), doi:10.1016/j.comnet.2009.07.013
15. Newsome, J., Shi, E., Song, D., Perrig, A.: The sybil attack in sensor networks: analysis & defenses (January 2004)
16. Xiu-Li, R., Wei, Y.: Method of Detecting the Sybil Attack Based on Ranging in Wireless Sensor Network. In: 5th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1–4 (2009), doi:10.1109/WICOM.2009.5302573
17. Su, C.-C., Chang, K.-M., Kuo, Y.-H., Horng, M.-F.: The new intrusion prevention and detection approaches for clustering-based sensor networks. In: IEEE Conference on Wireless Communication and Networking, vol. 4, pp. 1927–1932 (2005), doi:10.1109/ WCNC.2005.1424814
18. Liu, D., Ning, P., Li, R.: Establishing pairwise keys in distributed sensor networks. ACM Transactions on Information and System Security 8(1) (2005), doi:10.1145/1053283. 1053287
19. Hwang, J., Kim, Y.: Revisiting random key pre-distribution schemes for wireless sensor networks. In: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (2004), doi:10.1145/1029102.1029111
20. Camtepe, S.A., Yener, B., Yung, M.: Expander Graph based Key Distribution Mechanisms in Wireless Sensor Networks. In: IEEE International Conference on Communication, pp. 2262–2267 (2006), doi:10.1109/ICC.2006.255107
21. Sajedi, H., Jamzad, M.: Secure cover selection steganography. In: Park, J.H., Chen, H.-H., Atiquzzaman, M., Lee, C., Kim, T.-h., Yeo, S.-S. (eds.) ISA 2009. LNCS, vol. 5576, pp. 317–326. Springer, Heidelberg (2009)

22. Turner, C.: A steganographic computational paradigm for wireless sensor networks. In: International Conference on Innovations and Information Technology, pp. 258–262 (2009), doi:10.1109/IIT.2009.5413637
23. Du, W., Deng, J., Han, Y.S., Varshney, P., Katz, J., Khalili, A.: A Pairwise Key Predistribution Scheme for Wireless Sensor Networks. The ACM Transactions on Information and System Security (TISSEC) 8(2), 228–258 (2005)
24. Chen, C., Song, M., Hsieh, G.: Intrusion detection of Sinkhole attack in largescale wireless sensor network. In: WCNIS 2010, pp. 711–716 (2010)
25. Labraoui, N., Gueroui, M., Aliouat, M.: Secure DVHop localization scheme against wormhole attacks in wireless sensor networks. In: European Transactions on Telecommunications, doi:10.1002/ett.1532
26. Krontiris, I., Giannetsos, T., Dimitriou, T.: Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side. In: WiMob 2008, pp. 526–531 (2008)