International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-06

AN EFFICIENT APPROACH FOR REPLICA NODE DETECTION USING RANDOM KEY DISTRIBUTION IN WIRELESS SENSOR NETWORKS

M.Divya[1],
PG student
Computer Science and Engineering,
S.A Engineering College,
Chennai, India.

R.Geetha[2],
Associate Professor,
Computer Science and Engineering,
S.A Engineering College,
Chennai, India.

***Abstract*-Wireless sensor networks (WSN) are widely used in applications like military surveillance. Clone node attack is a major threat in wireless sensor network. Many approaches have been proposed for detecting clone attacks. A decentralized protocol which is based on a distributed hash table (DHT) detects the clone nodes using chord algorithm and constructs the overlay network. Here every node is assigned with a unique key which is verified by a witness node before transmitting data. A distributed detection protocol, known as randomly directed exploration (RDE), presents outstanding communication performance and minimal storage consumption for dense sensor networks. It is a location based node identification protocol. The group leader will generate a random number with time stamp to the available nodes that should be verified by the witness node to detect the cloned nodes. The distributed mechanism has been proposed to identify clone node attack, which also detects framing attack. In DHT and RDE, Inspector node identifies clone nodes but, this information may be modified by the malicious node during the transmission to other node which is to be avoided .Our work proves that, this can be achieved by using Random key distribution scheme. Here bloom filters are used to collect key usage data. Each and every sensor nodes randomly selects keys from the key pool where, key pool contains keys and key identifiers. Inspector node communicates with other node with the help of key discovery, which finds a common key in the set of key. For further communication use this secrete key and Initiator send action message correctly and maintain as trusted role with the help of Random key distribution.**

Index terms-Wireless Sensor Networks (WSN), Distributed Hash Table (DHT), Randomly Directed Exploration (RDE), Random key distribution

I. INTRODUCTION

Wireless sensor networks consist of autonomous device called sensors to monitor physical or environmental conditions. WSNs are mainly developed for military applications to track enemy and used for security detection. It is a collection of hundreds and thousands of resources with minimum cost. In general, sensor nodes are randomly scattered in the surveillance area working without their presence. Among many physical attacks, the node replica is a serious and dangerous one [1]. Because of production expenditure limitation, Sensor nodes are short of tamper resistance hardware components. Thus, an enemy can capture some nodes, extract code and all secrete credentials. Replica node uses this information to clone many nodes in the sensor network [6].Those cloned nodes can join freely in the sensor network as a legitimate node and then enlarge the adversary's capacities to operate the network maliciously. The adversary may collect all secret information from the sensor nodes and enlarge the clone node. The secret information such as ID's and Keys are collected from captured nodes and adversary creates some normal nodes as cloned node.

To overcome energy and memory demanding by quickly detect replicated nodes because many replicated nodes can multiply the damage to the network.

Clone node is detected by using two methods in previous work the first one is a decentralized, Key based caching protocol which is based on a distributed hash table (DHT) which is created to identify the cloned nodes. DHT detects replica node with high security and holds strong resistance against adversary's attacks. A distributed detection protocol,

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-06

known as randomly directed exploration is designed to provide efficient communication performance with sufficient detection probability for dense sensor networks. It is a location based node identification protocol. In sensor network, every node needs to know a neighbor list containing all neighbors IDs and locations and this should be stored temporarily. During the process an inspector detect clone node by compares its own neighbor list with the message's neighbor list. Finally, witness identified the cloned node and send evidence message to the entire node in the network.

Our work is extended by using Random key distribution scheme in DHT and RDE protocol. Normally initiator send an action message to all observers and every observer construct a claiming message with neighbor ID and Location and observer ID and Location, and then send this information to all nodes in the sensor network. Finally, Inspector node identifies clone node but, this information may be modified by the malicious observer during the transmission to other nodes which is to be avoided by using random key distribution scheme. In sensor network, every node is assigned with key to authenticate the nodes. The key is identified as clone or not by how often these keys are used by the nodes. Bloom filter is used by every node to count the number of times the key is used. Inspector verifies the count with predefined threshold. Then, the particular node is detected as a cloned node. This scheme only finds the clone key not the clone node [3].

Various methods have been proposed to detect replica attacks [1],[3],[4],[5],[7],[8],[9],[10]. These are important to detect the abnormal symptoms caused by replicas (e.g.: a node having same ID sending message at different locations). Clone attack [1],[2],[6] (also called Replica attack) is a dangerous physical attack in WSN's.

II. PRELIMINARY WORKS

In general, Replica node is detected by using three schemes: They are

A) Centralized detection method
B) Distributed detection method
C) Decentralized detection method

A) Centralized detection method

In this method, central parties have the responsibility for receiving the details of all the nodes and making judgments of node clone.

In a centralized detection scheme, each node sends a list of neighbor nodes details and their locations to a base station which is used to find cloned nodes. The SET protocol [4], falls into base station based techniques. SET protocol is used to reduce communication cost by constructing subsets. Each of the subsets has a subset leader and the leader collects member's information and forwards to the root of the subtree to detect cloned nodes. If the intersection of entire subsets of a subtree is empty, then there are no replicas in the subtree. The base station detects the replica nodes by calculating the intersection of any two received subtrees subset leader, sends node information to the base station and then to the root node of a randomly created subtree.

B) Distributed detection method

In this method, all nodes have the ability to cooperatively process the information and detect node clone in a distributed manner.

In a distributed detection scheme, The RDE protocol [5] is a location based node identification protocol. This technique falls into Witness –node based techniques. Each node only needs to create its own neighbor list contains neighbor ID's and location. To detect clone node in the sensor network, an inspector check its own neighbor list with its message's neighbor list .Finally protocol detect clone node in a dense sensor networks and consumes minimum memory during detection and presents outstanding communication performance.

C) Decentralized detection method

In this method, there is no central party for receiving the details of all the nodes and no controller to control, many external systems can communicate with each others in the network, and discarding one node could not affect the other nodes, only lost that particular node. It will not affect the whole network.

The DHT protocol, a decentralized protocol which is based on Key based caching and checking system developed to detect cloned nodes. DHT detects the clone nodes by using chord algorithm and constructs the overlay network. Here

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-06

every node is assigned with a unique key, ID and location which are verified by a witness node before transmitting data. If any nodes ID, Key is same as the previous nodes ID and key then, that node is detected as replica node. Then, witness node send an evidence message about that particular replica node to all the nodes in the network and remove the clone node from the sensor network.

Steps of node replication attack

1. Sensor nodes are scattered in the field.
2. Physically capture one sensor node.
3. Collects all secret credentials from particular sensor node.
4. Captured node is replicated by the adversary.
5. Deploy this cloned node at strategic positions.

III. SYSTEM MODEL

In DHT and RDE protocol, it contains initiator, observer, and inspector and witness node. This technique falls into witness node based technique. Initiator sends an action message to all nodes in the network. Action message contains action time, nonce and random seed. Then every observer create claiming message for every neighbor node. Claiming message includes neighbor ID, location and observer ID, location. A claiming message is transmitted to destination node, which will cache ID, location and check for replica node detection. Then, some intermediate nodes behave as an inspector to improve toughness against the adversary in an efficient way. An inspector is used to verify the claiming message. In the network, one inspector detects the clone node and become a witness and sends an evidence message to all the sensor nodes (send the ID and location of the replica node as an evidence message to the entire node in the network).

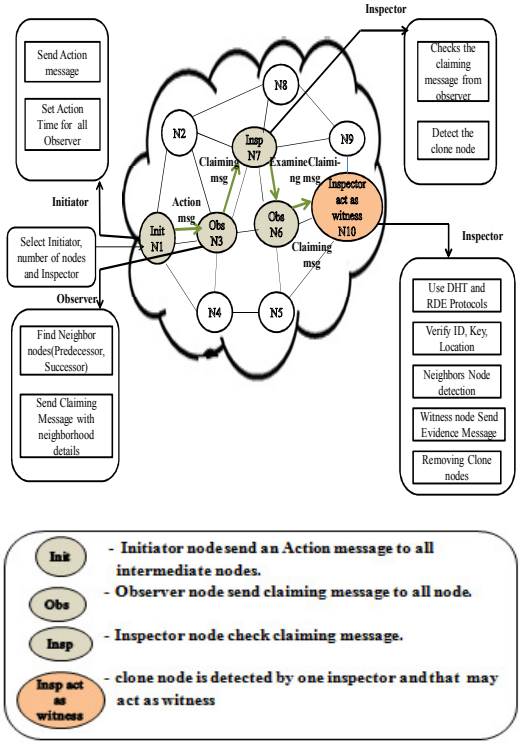

Fig.1. System architecture

In DHT and RDE, inspector node identifies clone node but, this information may be modified by the intruder and that node is treated as malicious observer. They try to frame innocent nodes by claiming wrong locations during the transmission to other nodes which is to be avoided by using the witness node, it can increase the detection rate of replica node. Our work proves that, this can be achieved by using random key distribution scheme. This is a key based transmission technique. Here every node is assigned with key to authenticate the nodes in the network. The key is identified as replica by how often these keys are used by the nodes. Bloom filter is used by every node to count the number of times the key is used. It is mainly used to collect key usage data. Each and every sensor nodes randomly selects a keys and key identifiers. Inspector node communicate with other node with the help of key discovery, that finds a common key in the set of key for further communication use this secret key. In sensor network, keys present on replicated nodes are

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-06

detected by how many times they are used to establish as true in the network. Inspector verifies the count with predefined threshold then, that particular node is identified as a cloned node. This scheme only finds the clone key not the clone node. Based on the cloned key, the cloned node is detected but with the help of DHT by using random key distribution replica node must be detected because, DHT will provide the information about the clone node ID, location and random key distribution provide the clone key with the help of these information, the replica node must be identified. This approach will avoid the intruder to create the replica node. Initiator must be maintained as trusted.

IV. PROPOSED WORK

As a condition, after identifying a cloned node with cloned key using random key distribution scheme in DHT protocol. Inspector detects a clone node and become a witness. Then, witness sends an evidence message to the entire node in the sensor network. But in our concept Bloom filter found the cloned keys and filter the keys then, the filter message is transmitted to inspector. The inspector act as witness will forward an evidence message to neighbor within the target zone then, it reach destination otherwise, if there is no neighbor within the target zone then forward message to many intermediate node .In the network some intermediate act as malicious node. By knowing cloned node ID, location and keys. Inspector should not forward message to that particular malicious node. This is a key based transmission technique.

Algorithm 1: Detect clone node
1: **Procedure**: Initiator
2**: Broadcast**- Action message
3: Action message← {Nonce, Random seed, Action time}
4: specify transmission time in action msg for sending every claiming message
5: **end procedure**
6: **Procedure:** Observer
7: **Receive** Action msg
8: **if** (msg nonce > last nonce) **then**
9: **check "**msg signature**"**
10: valid
11: Node operate as observer **then**
12: **Broadcast**: claiming message
13: Claiming message←{Neighbor ID, Neighbor Location, Observer ID, Observer Location}
14: **Destination node receives** claiming message
15: **inspect claiming message** (Destination act as an inspector)
16: **return** NIL (reach destination)
17: else if
18: forward msg to next node with Id
19: same ID at different Location
20: Inspector found clone and become a witness
21: **Broadcast** evidence message
22: evidence message ←cloned node {ID, Loc}
23: Detected clone node
24: **end procedure**

Algorithm 2: DHT using Random Key Distribution approach
1: **Input:** Detected clone node
2: Inspector become witness and detect clone node **(use Algorithm 1)**
3**: If** found clone **then**
4: Witness **broadcast** evidence msg← {ID, Loc, and Nonce}
5: insert keys to all nodes
6: Bloom filter← count the number of times the key is used
7: Inspector receives filter
8: verify the count within predefined threshold value
9: **if** (key value > threshold value) **then**
10: found cloned key
11: **else**
12: forward keys to next node with msg
13: **if** neighbor within the target zone **then**
14**: return** NIL (reach destination)
15: **if** no neighbor within the target zone **then**
16: forward msg to many intermediate nodes
17: Intermediate act as malicious node **then**
18: Inspector should not forward msg to that particular malicious node
19: cloned keys and nodes identified by Bloom filter and witness
20: Inspector forward msg to correct node
21: **Output:** Trustworthy transmission of clone node information.

A) Initialization

To start node replica detection, initiator broadcast an action message including message nonce, Random seed, and set action time for all observer. The nonce is proposed to

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-06

avoid DoS attack by repeating broadcasting action message which is to prevent adversaries from launching a DoS attack.

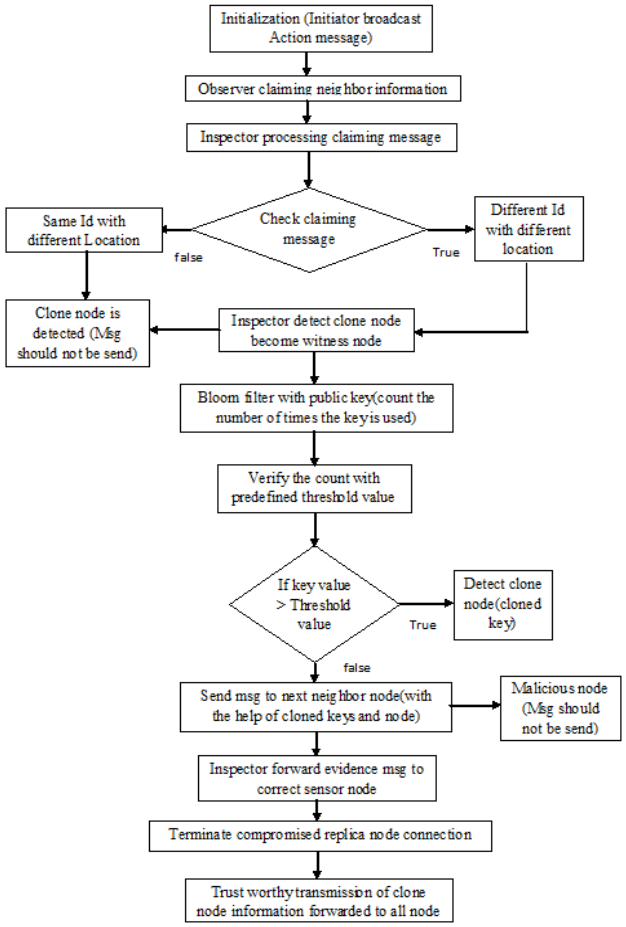

Fig.2. Stages of proposed operation

B) Observer claiming neighbor information

A neighbor receives an action message and verifies, if the message nonce is greater than the previous nonce and check for message signature is valid or not. If both are valid then, the node updates the nonce and store the random seed. At the designated action time the node operate as an observer and generate claiming message and transmits it to all nodes including neighbor ID, location and observer ID, location. Destination will cache Id-location pair and check for replica node detection acting as an inspector and some intermediate nodes also act as inspector to improve resilience against adversary in an efficient way. Inspector detect clone by node having same ID at different location and act as witness and send evidence message to all node and avoid replica node communication in the network.

C) Bloom filter

A Bloom filter [3] is an estimated representation of set that supports membership queries. Bloom filter is used by every node to identify the key of the node is clone or not. It counts the number of times the key is used than filters the keys and the filter is transferred to inspector. Then inspector verify the count of keys with threshold value, the particular node is identified as clone. In this scheme, it finds only the replica key not the replica node.

V. CONCLUSION

In DHT and RDE protocol, Inspector node identifies clone nodes but, this information may be modified by the malicious observer and they try to frame innocent nodes by claiming wrong locations during the transmission to other node which is to be avoided. Our work proves that, this can be achieved by using random key distribution scheme in DHT protocol. In this, bloom filter is used to identify the cloned keys by counting the number of times the key is used. Then, filter is transferred to the inspector which will verify the count with the predefined threshold, the particular node is found to be a cloned node. This scheme finds only the cloned key. Then, inspector detects replica node become witness and send evidence message to all nodes in the network. In this, keys are used for security purpose. Combination of DHT and Random key distribution scheme provides more security and detects the clone node efficiently.

ACKNOWLEDGMENT

I must thank, first and foremost my internal guide Mrs.R.Geetha, M.E, (Ph.D) Associate Professor, Department of computer science and Engineering, Dr.G.Umarani Srikanth, M.E, Ph.D Head of the Department, PG Studies and project coordinator Mr. C.Balakrishnan, M.E, (Ph.D) Assistant professor, PG studies without whose guidance and patience, this dissertation would not be possible. I am also thankful to project panel members and other professors of the Department

of Computer science and Engineering for their continuous encouragement and ideas.

REFERENCES

[1] B. Parno, A. Perring, and V. Gligor, "Distributed detection of node replication attacks in sensor networks", in proc. IEEE Symp. Security Privacy, pp.49-63, May 2005.

[2] K. Cho, M. Jo, T. Kwon, Chen, H-H. Fellow, and Hoon Lee, D, "Classification and Experimental Analysis for Clone Detection Approaches in wireless sensor networks", IEEE System journal, Vol. 7, No. 1, March 2013.

[3] R. Brooks, P.Y. Govindaraju, M. Pirretti, N. Vijay Krishna and M.T. 7, "On the Detection of Clones in Sensor Networks Using Random Key Predistribution", IEEE Transaction on System, Man and Cybernetics, Part C, Vol. 37, No. 6, November 2007.

[4] H. Choi, S. Zhu and T.F. La porta, "SET: Detecting node clones in sensor networks" Security and privacy in communications networks and the workshops. Secure comm., pp.341-350, September 2007.

[5] Z. Li and G. Gong "Randomly directed exploration: An efficient node clone detection protocol in wireless sensor networks", Mobile Adhoc and sensor systems, pp.1030-1035, October 2009.

[6] M. Conti, R. Di, Pietro, L. Vincenzo Mancini, and A. Mei, "Distributed Detection of Clone Attacks in Wireless Sensor Networks", IEEE Transaction on Dependable and secure computing., Vol. 8, No. 5, September 2011.

[7] Y. Zeng, J. Cao, S. Zhang, S. Guo and L. Xie, "Random-walk Based Approach to Detect Clone Attacks in wireless sensor networks", IEEE Journal on selected areas in Communications., Vol. 28, No. 5, June 2010.

[8] C-M. Yu, Y-T. Tsou, C-S. Lu and S-Y. Kuo, "Localized Algorithm for Detection of Node Replication Attacks in Mobile Sensor Networks", IEEE Transaction on Information forensics and security, Vol. 8, No. 5, May 2013.

[9] J-W. Ho, M. Wright and S-H. Das, "Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks using Sequential Hypothesis Testing", IEEE Transaction on Mobile Computing', Vol.10, No.6, June 2011.

[10] B. Zhu, S. Setia, S. Jajodia, S. Roy and L. Wang, "Localized Multicast: Efficient and Distributed Replica Detection in Large-Scale sensor networks", IEEE Transaction on Mobile Computing., Vol.9, No.7, July 2010.