International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Enhanced Distributed Detection Protocol for Node Replication Attack

Aiswaria E S

PG Student , Department of Computer Science and Engineering, Malabar College of Engineering, Cheruthuruthy,Thrissur

Abstract: ***Wireless sensor networks are harmed to the node clone, and different distributed protocols have been proposed to detect this attack. However, they require too strong assumptions to be practical for randomly deployed sensor networks. Here, two new node clone detection protocols with different tradeoffs on network conditions and performance are proposed. The first one is based on a DHT concept which abbreviated as distributed hash table, by which a fully decentralized, key-based caching and checking system is constructed to catch cloned nodes effectively. The protocol performance on efficient storage consumption and high security level is theoretically deducted through a probability model, and the resulting equations, with necessary modification for real application, are supported by the simulations. But the DHT-based protocol incurs similar communication cost as previous techniques, it may be considered a little high for some scenarios. To overcome communication cost problem our second approach RDE/DDE distributed detection protocol, named randomly directed exploration, presents good communication performance for dense sensor networks, by a probabilistic directed forwarding technique along with random initial direction and border determination. The simulation results uphold the protocol design and show its efficiency on communication overhead and satisfactory detection probability.***

Keywords: wireless sensor networks (wsn), distributed hash table, randomly directed exploration

1. Introduction

Wireless sensor networks (WSNs) have gained a great deal of attention in the past decade due to their wide range of application areas and formidable design challenges. In general, wireless sensor networks consist of hundreds and thousands of low-cost, resource-constrained, distributed sensor nodes, which usually scatter in the surveillance area randomly, working without attendance. If the operation environment is hostile, security mechanisms against adversaries should be taken into consideration. Among many physical attacks to sensor networks, the node clone is a serious and dangerous one . Because of production expense limitation, sensor nodes are generally short of tamper-resistance hardware components; thus, an adversary can capture a few nodes, extract code and all secret credentials, and use those materials to clone many nodes out of off-the-shelf sensor hardware. Those cloned nodes that seem legitimate can freely join the sensor network and then significantly enlarge the adversary's capacities to manipulate the network maliciously. For example, those vicious nodes occupy strategic positions and cooperatively corrupt the collected information. With a large number of cloned nodes under command, the adversary may even gain control of the whole network. Furthermore, the node clone will exacerbate most of inside attacks against sensor networks. A wireless sensor network consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, pressure, sound, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding. Wireless sensor networks are vulnerable to the node clone, and several distributed protocols have been proposed to detect this attack. However, they require too strong assumptions to be practical for large-scale, randomly deployed sensor networks. Advances in technology have made it possible to develop sensor nodes which are compact and inexpensive. They are mounted with a variety of sensors and are wireless enabled. Once sensor nodes have been deployed, there will be minimal manual intervention and monitoring. But, when nodes are deployed in a hostile environment and there is no manual monitoring, it creates a security concern. Nodes may be subjected to various physical attacks. The network must be able to autonomously detect, tolerate, and/or avoid these attacks. One important physical attack is the introduction of cloned nodes into the network. In this paper two node clone detection protocols are introduced via distributed hash table and randomly directed exploration to detect node clones. The former is based on a hash table value which is already distributed and provides key based facilities like checking

and caching to detect node clones. The later one is using probabilistic directed forwarding technique and border determination.

2. Objective

The low-cost of off-the-shelf hardware components in unshielded sensor-network nodes leave them vulnerable to compromise. With a little effort, the adversary can capture nodes, analyze and replicate them and surreptitiously insert these replicas at strategic locations within the network. These attacks have severe consequences and allow the adversary to corrupt network data or even disconnect significant parts of the network. Previous node replication detection schemes depend primarily on centralized mechanisms with single points of failure, or on neighborhood voting protocols that fail to detect distributed replications. To address these fundamental limitations, two new algorithms based on emergent properties. The first property is that arise only through the collective action of multiple nodes. The second property is Randomized multicast distributed node location information to randomly-selected witnesses, exploiting the birthday paradox to detect replicated nodes while line-selected multicast uses the topology of the network to detect replication. Both of the algorithms provide globally-aware, distributed node replica detection and line-selected multicast displays particularly strong performance characteristics. The emergent algorithms also represent a promising new approach to sensor network security. Moreover, the results naturally extend to other classes of networks in which nodes can be captured, replicated and re-inserted by an adversary.

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. 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).

3. Problem Definition

The earliest method to detect node clones was prevention schemes and key plays the main role which provided to nodes by mobile trusted agents. The private key of node comprises of location and identity. But the problems arise here are attackers may takes some time to compromise the nodes (compromising time) in the network. As the compromising time decreases the number of clone nodes increases thus badly affects the security of the network. And also prevention scheme is applicable to only some specific applications. The assumption made on trusted agents is not too strong .

In the centralized detection method a base station is connected to each node. Each node sends a list of its neighbor nodes and location to base station. The communication cost is limited by constructing subsets of nodes. Even though communication cost is reduced the life time expectancy of the network is decreased due to the communication burden of the nodes near to the base station.

The main aim of the research is the progress of efficient wireless sensor networks with high security point and holds strong resistance against adversary s assault. It is projected to provide highly efficient communication presentation with adequate detection probability for bulky sensor networks. With many physical attacks to sensor networks, the node clone is a serious and dangerous one to Production expense limitation, sensor nodes are generally short of tamper-resistance hardware components. Thus, an adversary can capture a few nodes, extract code and all secret testimonials and use that equipment to clone many nodes out of off-the-shelf sensor hardware. Those cloned nodes seem that legitimate can freely join the sensor network and then significantly enlarge the adversary capacities to direct the network maliciously. Wireless Sensor Network (WSN) with spatially distributed autonomous are used to monitor physical or environmental conditions such as temperature, sound, pressure, etc. The modernized Wireless Sensor Networks are bi-directional enabling the control of sensor activity. The Wireless Sensor Networks are developed such that they are useful in military applications as battlefield surveillance. Now a day s these networks are also used in many industrial consumer applications like industrial process monitoring, health monitoring etc. Sensor nodes are small computers usually consisting of a processing unit with an average computational power, limited memory, sensors or MEMS, a communication device (usually radio transceivers or alternatively optical) and a power source usually in the form of a battery.

4. Literature Survey

4.1 Distributed Detection of Node Replication Attacks in Sensor Networks

This research paper is proposed by. B. Parno, A. Perrig, and V. Gilmore proposes a effective detection method called Randomized, Authentic, Efficient, Distributed protocol to detect node replication attack in wireless sensor network. The low-cost, off-the-shelf hardware components in unshielded sensor-network nodes leave them vulnerable to compromise. With little effort, an adversary may capture nodes, analyze and replicate them, and surreptitiously insert these replicas at strategic locations within the network. Such attacks may have severe consequences; they may allow the adversary to corrupt network data or even disconnect significant parts of the network. Previous node replication detection schemes depend primarily on centralized mechanisms with single points of failure, or on neighborhood voting protocols that fail to detect distributed

replications. To address these fundamental limitations, two new algorithms is proposed based on emergent properties (Gligor (2004)), i.e., properties that arise only through the collective action of multiple nodes. Randomized multicast distributes node location information to randomly-selected witnesses, exploiting the birthday paradox to detect replicated nodes, while line-selected multicast uses the topology of the network to detect replication. Both algorithms provide globally-aware, distributed node-replica detection, and line-selected multicast displays particularly strong performance characteristics. The emergent algorithms represent a promising new approach to sensor network security; moreover, our results naturally extend to other classes of networks in which nodes can be captured, replicated and re-inserted by an adversary.

4.2 Looking up data in P2P systems

This research paper is proposed by H. Balakrishnan, M. F. Kaashoek, D. Karger, R. Morris, and I. Stoica. The main challenge in P2P computing is to design and implement a robust distributed system composed of inexpensive computers in unrelated administrative domains. The participants in a typical P2P system might be home computers with cable modem or DSL links to the Internet, as well as computers in enterprises. Some current P2P systems have reported tens of thousands of simultaneously active participants, with half a million participating machines over a week-long period. P2P systems are popular and interesting for a variety of reasons:

1) The barriers to starting and growing such systems are low, since they usually don't require any special administrative or financial arrangements, unlike with centralized facilities.
2) P2P systems suggest a way to aggregate and make use of the tremendous computation and storage resources that otherwise just sit idle on computers across the Internet when they are not in use.
3) The decentralized and distributed nature of P2P systems gives them the potential to be robust to faults or intentional attacks, making them ideal for long-term storage as well as for lengthy computations.

P2P computing raises many interesting research problems in distributed systems. In this short paper we will look at one of them, the lookup problem: How do you find any given data item in a large P2P system in a scalable manner, without any centralized servers or hierarchy? This problem is at the heart of any P2P system. It is not addressed well by most systems in popular use, and it provides a good example of how the challenges of designing P2P systems can be addressed. The recent algorithms developed by several research groups for the lookup problem present a simple and general interface, a Distributed Hash Table (DHT). Data items are inserted in a DHT and found by specifying a unique key for that data. To implement a DHT, the underlying algorithm must be able to determine which node is responsible for storing the data associated with any given key. To solve this problem, each node maintains information (e.g., the IP address) of a small number of other nodes ("neighbors") in the system, forming an overlay network and routing messages in the overlay to store and retrieve keys. One might believe from recent news items that P2P systems are good for illegal music swapping and little else, but this would be a rather hasty conclusion. The distributed hash table, for example, is increasingly finding uses in the design of robust, large-scale distributed applications. It appears to provide a general-purpose interface for location-independent naming upon which a variety of applications can be built. Furthermore, distributed applications that make use of such an infrastructure inherit robustness, ease of operation, and scaling properties. A significant amount of research effort is now being devoted to investigating these ideas.

4.3 Location-based compromise tolerant security mechanisms for wireless sensor networks

This research paper proposed is by Y. Zhang,W. Liu,W. Lou, and Y. Fang proposes a new cryptographic concept called pairing. Node compromise is a serious threat to wireless sensor networks deployed in unattended and hostile environments. To mitigate the impact of compromised nodes, we propose a suite of location-based compromise-tolerant security mechanisms. Based on a new cryptographic concept called pairing, we propose the notion of location-based keys (LBKs) by binding private keys of individual nodes to both their IDs and geographic locations. We then develop an LBK-based neighborhood authentication scheme to localize the impact of compromised nodes to their vicinity. We also present efficient approaches to establish a shared key between any two network nodes. In contrast to previous key establishment solutions, our approaches feature nearly perfect resilience to node compromise, low communication and computation overhead, low memory requirements, and high network scalability. Moreover, we demonstrate the efficacy of LBKs in counteracting several notorious attacks against sensor networks such as the Sybil attack, the identity replication attack, and wormhole and sinkhole attacks. Finally, we propose a location-based threshold-endorsement scheme, called LTE, to thwart the infamous bogus data injection attack, in which adversaries inject lots of bogus data into the network. The utility of LTE in achieving remarkable energy savings is validated by detailed performance evaluation.

4.4 LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks

This research paper is proposed by S.Zhu,S.Setia, And S.Jajodia proposes an LEAP (Localized Encryption and Authentication Protocol), a key management protocol for sensor networks that is designed to support in-network processing, while at the same time restricting the security impact of a node compromise to the immediate network neighborhood of the compromised node. The design of the protocol is motivated by the observation that different types of messages exchanged between sensor nodes have different security requirements, and that a single keying mechanism is not suitable for meeting these different security requirements. LEAP supports the establishment of four types of keys for each sensor node – an individual key shared with the base station, a pair wise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a global key shared by all the nodes in the network.

LEAP also supports (weak) local source authentication without precluding in-network processing. Our performance analysis shows that LEAP is very efficient in terms of computational, communication, and storage costs. We analyze the security of LEAP under various attack models and show that LEAP is very effective in defending against many sophisticated attacks such as HELLO flood attacks, node cloning attacks, and wormhole attacks. LEAP includes support for multiple keying mechanisms. The design of these mechanisms is motivated by the observation that different types of messages exchanged between sensor nodes have different security requirements, and that a single keying mechanism is not suitable for meeting these different security requirements. Specifically, LEAP supports the establishment of four types of keys for each sensor node – an individual key shared with the base station, a pair wise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a global key shared by all the nodes in the network. Moreover, the protocol used for establishing these keys for each node is communication- and energy-efficient, and minimizes the involvement of the base

5. Proposed Approach

In this paper two innovative, practical node clone detection protocols with difference tradeoffs on network conditions and performance. The first protocol is based on the distributed hash table (DHT), by which a fully decentralized, key-based caching and checking system is constructed to effectively catch cloned nodes. The protocol performance on security level as well as memory consumption is theoretically deducted through a probability model, and the resulting equations, with necessary adjustment for real application, are supported by the simulations. In accordance with our analysis, the comprehensive experimental results show that the DHT-based protocol can detect node clone with high security level and holds strong resistance against adversary's attacks.

The second protocol, named randomly directed exploration, is intended to provide highly efficient communication performance with adequate detection probability for dense sensor networks. In this protocol, initially nodes send claiming messages containing neighbor-list with a maximum hop limit to randomly selected neighbors; then the subsequent message transmission is guided by a probabilistic directed technique to both roughly maintain a line property through the network and provide sufficient randomness for better performance on communication and resilience against the adversary. In addition, a border determination mechanism is proposed to further reduce communication payload. During forwarding messages, intermediate nodes explore claiming messages for node clone detection. By design, this protocol consumes almost minimal memory, and the simulations demonstrate that it outperforms all other detection protocols in terms of communication cost, while the detection probability is competitive.

In Enhanced distributed detection protocol for node replication attack, DHT and RDE is used to catch the cloned node effectively. Here as the first step initialization is done to active all nodes in the wireless sensor network. After initialization all nodes in the wireless sensor network will become active. The source node will make a connection with the sink node for the proper transmission of the message. When message is send from source node to sink node DHT and RDE is used to check whether clone is present or not. So security purpose all nodes information in wireless sensor network are stored by its neighboring nodes and therefore these two protocol are said to be decentralized. After initialization, one node is set as an observer node and observer will generate claiming message and it is send to its neighboring nodes . All the neighboring nodes will send their IP, node name, location to observer. observer in turn send some token no to the nodes(DHT) and save it into hash table. A claiming message will be forwarded to its destination node via several intermediate nodes. Only those nodes in the network (i.e., the source node, intermediate nodes, and the destination node) need to process a message, whereas other nodes along the path simply route the message to temporary targets. During handling a message the node acts as an inspector if one of the following conditions is satisfied:

1) This node is the destination node of the claiming message.
2) The destination node is one of the successors of the node.

During the processing, inspector node , compares its own neighbor-list to the neighbor-list in the message, checking if there is a clone. Similarly, if detecting a clone, the witness node will broadcast an evidence message to notify the whole network such that the cloned nodes are expelled from the sensor network

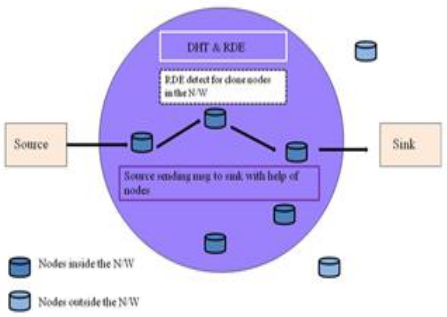

Figure 1: Architectural diagram of clone node detection

6. Algorithm

The proposed algorithm works with the following steps;
Step 1 . Start
Step 2 . Initialize nodes, node connection, protocol and Links
Step 3 . Select a node for initiator
Step 4 . Initiator sends a broad case message and client nodes send a replay message through the connection
Step 5 . Call the function On The Node Clone Detection
Step 6. stop

On The Node Clone Detection

Step 1 . Initialise variables
Step 2 . Select one node from node table
Step 3 .Node send a request message to Neighbour nodes to prove their identity

Step 4 . Neighbouring node send a claim message for authentication
Step 5 . If whether a clone node is found call the function Find Inspectors in a group of nodes
Step 6 . Sleep 2 minutes call the function On The Node Clone Detection until stop.

Find Inspectors
Step 1 . Select a node from group of channel as Inspector
Step 2 . Inspector node sends broad cast message to its successors to prove their identity
Step 3 . Neighbouring nodes send back their identity and Inspector node check whether a clone is found or not
Step 4 . If found make it a Witness node and board cast evidence to neighbouring nodes
Step 5 . Reset Identity and return.

7. Conclusion

Sensor nodes lack tamper-resistant hardware and is subject to the node clone attack. In this research paper, two distributed detection protocols are proposed. First one is based on a distributed hash table which forms a Chord overlay network and provides the key-based routing caching and checking facilities for clone detection. Second one uses probabilistic directed technique to achieve efficient communication overhead for satisfactory detection probability. While the DHT-based protocol provides high security level for all kinds of sensor networks by one deterministic witness and additional memory-efficient, probabilistic witnesses. DHT-based protocol can effectively detect clone for general sensor networks with high security level and efficient storage consumption, while its communication cost is in the same order of magnitude with previous detection schemes sensor networks e.g., virtual cord protocol. As more and more low-bit rate compression standards for video are emerging and with the progress of wireless technology .The Randomly Directed Exploration presents outstanding communication performance with minimal storage consumption for denser sensor networks. From exploration protocol outperforms all other distributed detection protocols in terms of communication cost and storage requirements, while its detection probability is satisfactory, higher than that of line selected multicast scheme. In addition, all nodes only need to know their direct neighbour s information and inherent routing technique delivers messages in an efficient way to cover great range of the network.

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, and Y. Fang, "Location-based compromise tolerant 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

Author Profile

Aiswaria E S, received B. Tech. degree in Computer Science and Engineering from Malabar College of Engineering, Calicut University, in 2013. Currently she is doing M. Tech. in Computer Science, from Malabar College of Engineering, Thrissur , India.