International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438..1

Review on Detection of Clone Attacks inWireless Sensor Networks

Nikita R. Kitey[1], Dr. M. S. Ali[2]

[1]ME (CSE) II Year,, Prof. Ram Meghe College of Engineering and Management, Amravati University, Amravati, India

[2]Prof. Ram Meghe College of Engineering and Management, Amravati University, Amravati, India

Abstract: ***Wireless Sensor networks (WSN) is an emerging technology and have great potential to be employed in critical situations like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios. Wireless sensor networks are often deployed in hostile environments, where an adversary can physically capture some of the nodes. Once a node is captured, the attacker can re-program it and replicate the node in a large number of clones, thus easily taking over the network. The detection of node replication attacks in a wireless sensor network is therefore a fundamental problem. A few distributed solutions have recently been analyzed. Here we propose two novel node clone detection protocols with different tradeoffs on network conditions and performance. The first one is based on a distributed hash table (DHT), by which a fully decentralized, key-based caching and checking system is constructed to catch cloned nodes effectively. Our second distributed detection protocol, named randomly directed exploration. It presents good communication performance for dense sensor networks, by a probabilistic directed forwarding technique along with random initial direction and border determination.***

Keywords: Wireless sensor networks, clone, distributed detection, DHT- Distributed hash table, Randomly directed exploration

1. Introduction

Wireless sensor networks are becoming increasingly important for a wide variety of applications such as factory instrumentation, climate control, environmental monitoring and building safety. It has gained a great deal of attention in the past decade due to their wide range of application areas. 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. As sensor networks become cheaper and more commoditised, they will become attractive to home users and small businesses, and for other new applications. A typical sensor network has a large number of small nodes that use wireless peer-to-peer communication to form a self-organized network [1]. They use multi-hop routing algorithms based on dynamic network and resource discovery protocols. To keep costs down and to deal with limited battery energy, nodes have fairly minimal computation, communication, and storage resources. They do not have tamper-proof hardware. We can thus expect that some small fraction of nodes in a network may be compromised by an adversary over time.Sensor nodes typically have a limited amount of memory, often on the order of a few kilobytes [2]. Thus, any protocol requiring a large amount of memory will be impractical. If the operation environment is unfriendly, security mechanisms against adversaries should be taken into consideration.

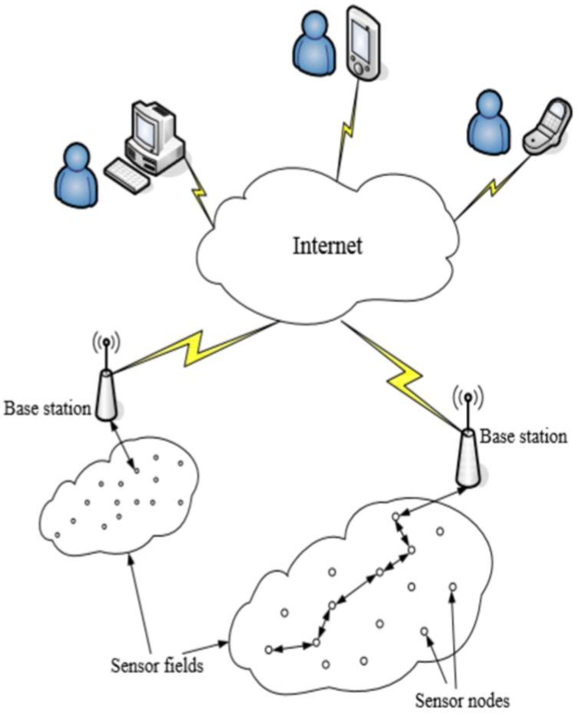

Figure : Accessing WSN using internet

2. Motivation

One of the major challenges wireless sensor networks face today is security. While the deployment of sensor nodes in an unattended environment makes the networks vulnerable to a variety of potential attacks, the inherent power and memory limitations of sensor nodes makes conventional security solutions unfeasible. 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. 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. The attempt is to detect the node clone in wireless sensor networks by using distributed hash table and randomly directed exploration.

3. Literature Review

Previous node replication detection schemes depend primarily on centralized mechanisms with single points of failure, or on neighbourhood voting protocols that fail to detect distributed replications. To address these fundamental limitations, Bryan Parno, Adrian Perrig and Virgil Gligor [5] propose two new algorithms based on emergent properties [18]. Randomized Multicast (RM) distributes node location information to randomly-selected witnesses, with the advantage of birthday paradox to detect replicated nodes, while Line-Selected Multicast (LSM) 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. Authors show that algorithms represent a promising approach to sensor network security,results naturally extend to other classes of networks in which nodes can be captured, replicated and re-inserted by an adversary.Randomized multicast- for detecting replication of nodes.Line selected multicast- To reduce the communication costs of randomized multicast protocol. To obtain acceptable detection probability, nodes have to buffer a great many of messages and every node is aware of all other nodes' existence, which is a very strong assumption for large-scale sensor net- works hence limits their applicability. Argue is security of such networks will increasingly depend on emergent algorithms. Cost considerations and unattended deployment will always leave individual sensors vulnerable to compromise.

Hari Balakrishnan, M. Frans Kaashoek, David Karger, Robert Morris, Ion Stoica[6] describes looking up data in P2P systems. The main challenge in P2P computing is to design and implement a robust distributed system composed of inexpensive computers in unrelated administrative domains. P2P systems that have no centralized control or hierarchical organization, 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. Challenges in designing the P2P systems can be addressed by a good example. 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 ("neighbours") in the system, forming an overlay network and routing messages in the overlay to store and retrieve keys.

In P2P, 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. P2P systems suggest a way to aggregate and make use of the tremendous computation and storage resources. The decentralized and distributed nature of P2P systems gives them the potential to be robust to faults or intentional attacks. In summary, these P2P lookup systems have many aspects in common, but comparing them also reveals a number of issues that will need further investigation or experimentation to resolve. They all share the DHT abstraction in common, and this has been shown to be beneficial in a range of distributed P2P applications. With more work, DHT's might well prove to be a valuable building block for robust, large-scale distributed applications on the Internet.

Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang [7] propose Location based compromise tolerant security mechanism for wireless sensor networks. Problem definition is to resist from various insider attacks, to resist from Sybil attack or identify replication attack and to design a compromise-tolerant security design. Without legitimate location based key, a malicious node can't successfully finish mutual authentication. Internal adversaries can induce arbitrary and seemingly authentic data reports into the network. A data report should be co-signed by nodes for it to be considered authentic. The sensor nodes can't move. Still have some problem about routing attack.The identity-based cryptography is used in their protocol such thatnodes'privatekeysareboundedbybooththeiridentitiesand locations.Oncenodesaredeployed,sometrustedmobileagents travel around the sensor network and issue the location-based keys to sensor nodes. Since those location-based keys cannot be used in nodes at other locations, node clone attack is inherently frustrated.

Sencun Zhu, Sanjeev Setia, Sushil Jajodia [8] describe LEAP (Localized Encryption and Authentication Protocol), a key management protocol for sensor networks that is designed to support in-network processing. LEAP supports the establishment of four types of keys for each sensor node – an individual key shared with the base station, a pairwise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a group key that is shared by all the nodes in the network. The protocol used for establishing and updating these keys is communication and energy-efficient, and minimizes the involvement of the base station. LEAP also includes an efficient protocol for local broadcast authentication based on the use of one-way key chains. A salient feature of the authentication protocol is that it supports source authentication without precluding in-network processing. LEAP is very efficient in computation, communication, and storage. Here analyzed the security of LEAP under various attack models. It gives efficient security mechanisms for large scale distributed sensor networks.

Ross Anderson, Haowen Chan and Adrian Perrig [9] propose Key Infection: Smart Trust for Smart Dust. The goal is to make sensors so small and cheap that they can be distributed in large numbers over an area by random scattering. The key distribution problem can be dealt with in environments with a partially present, passive adversary: a node wishing to communicate securely with other nodes simply generates a symmetric key and sends it in the clear to its neighbours. Despite the apparent insecurity of these primitive, mechanisms are used for key updating, multipath secrecy amplification and multihop key propagation to build up extremely resilient trust networks where at most a fixed proportion of communications links can be eavesdropped.Those prevention schemes might be useful on particular applications, but their assumptions as trusted mobile agents and initial trust are too strong to be applicable in general cases.

Mauro Conti, Roberto Di Pietro and Luigi V. Mancini and Alessandro Mei [10] propose a Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks. In this paper first, analyze the desirable properties of a distributed mechanism for the detection of node replication attacks. Second, they show that the known solutions for this problem do not completely meet our requirements. Third, they propose a new Randomized, Efficient, and Distributed (RED) protocol for the detection of node replication attacks and it is completely satisfactory with respect to the requirements. Extensive simulations also show that this protocol is highly efficient in communication, memory, and computation, that it sets out an improved attack detection probability. In particular, authors have introduced the preliminary notion of ID-obliviousness and area-obliviousness that conveys a measure of the quality of the node identity replica detection protocol, i.e., its resilience to an active attacker. Moreover, it is indicated that the overhead of such a protocol should not only be small, but also evenly distributed among the nodes, both in computation and memory. Main contribution is the a Randomized, Efficient, and Distributed (RED) protocol that is able for detecting node replication attacks. They compared RED to LSM through extensive simulations. These simulations proved that the overhead introduced by RED is low and almost evenly balanced among the nodes, while these properties are not provided by LSM. Finally, RED is both ID-oblivious and area-oblivious and also shows a dramatic improvement in detection capability.

Bo Zhu, Venkata Gopala Krishna Addada, Sanjeev Setia, Sushil Jajodia and Sankardas Roy [11] propose Efficient Distributed Detection of Node Replication Attacks in Sensor Networks. Authors present a novel distributed protocol for detecting node replication attacks that takes a different approach for selecting witnesses for a node. In their approach, i.e. Localized Multicast, the witness nodes for a node identity are randomly selected from the nodes that are located within a geographically limited region (referred to as a cell). The approach first deterministically maps a node's ID to one or more cells, and then uses randomization within the cell(s) to increase the resilience and security of the scheme. Localized Multicast approach is designed for two variants, first is Single Deterministic Cell (SDC) and second is Parallel Multiple Probabilistic Cell (P-MPC). Approach combines deterministic mapping (to reduce communication and storage costs) with randomization to increase the level of resilience to node compromise. Theoretical analysis and empirical results show that schemes are more efficient in terms of communication and memory costs. Moreover, the probability of detecting node replicas is much higher and security is achieved.Their approaches rely on the nodes' knowledge of the general deployed geography of sensor networks, cannot be guaranteed generally.

Heesook Choi, Sencun Zhu, Thomas F. La Porta [12] propose a new effective and efficient scheme, called SET, to detect clone attacks. The key idea of SET is to detect clones by computing set operations (intersection and union) of exclusive subsets in the network. First, SET securely forms exclusive unit subsets among one-hop neighbors in the network in a distributed way. This secure subset formation also provides the authentication of nodes' subset membership. SET then employs a tree structure to compute non-overlapped set operations and integrates interleaved authentication to prevent unauthorized falsification of subset information during forwarding. Randomization is used to further make the exclusive subset and tree formation unpredictable to an adversary. SET is composed of four components: formation of exclusive subsets, authentication of subset covering, distributed set computation on subset trees, and preservation of reliable set operations on the tree. The randomization schemes used in SET enable resilient and efficient detection, while providing distributed load sharing among nodes in the network. They show the reliability and resilience of SET by analyzing the probability that an adversary may effectively obstruct the set operations. The proposed scheme is more efficient from both communication and memory cost standpoints. However, in order to prevent malicious nodes, an authenticated subset covering protocol has to be performed, which considerably increases the communication burden and complicates the detection procedure

Haowen Chan Adrian Perrig Dawn Song [13] gives Random Key Pre-distribution Schemes for Sensor Networks. Key establishment in sensor networks is a challenging problem because asymmetric key cryptosystems are unsuitable for use in resource constrained sensor nodes, and also because the nodes could be physically compromised by an adversary. Here present three new mechanisms for key establishment using the framework of pre-distributing a random set of keys to each node. First, in the q-composite keys scheme, they trade off the unlikeliness of a large-scale network attack in order to significantly strengthen random key pre-distribution's strength against smaller-scale attacks. Second, in the multipath-reinforcement scheme, authors show how to strengthen the security between any two nodes by leveraging the security of other links. Finally, they present the random-pairwise keys scheme, which perfectly preserves the secrecy of the rest of the network when any node is captured, and also enables node-to-node authentication and quorum-based revocation. Each of these three schemes represents a different trade- off in the design space of random key protocols. The (2-hop) multipath reinforcement schemeimproves security at the cost of network communication overhead.

Richard Brooks, P. Y. Govindaraju, Matthew Pirretti, N. Vijaykrishnan and Mahmut T. Kandemir [14] present a hypothesis testing approach to detecting cloning attacks in sensor networks using random key predistribution. Bloom filters collect key usage data securely and efficiently. A server uses this data to create a key usage histogram. They derived the key usage probability distribution, and showed how the false positive rate defines the key usage threshold. Keys whose use exceeds the threshold value are considered cloned and erased from the network. This is a method for identifying the keys that are used by cloned nodes. The system can recover from a cloning attack by terminating connections using cloned keys. The algorithm can remove all cloned keys from the network.Integrating methods into random key predistribution security approaches will greatly reduce system vulnerability to cloning attacks.Inthe protocol, every node reports its keys to a base station, and then thebasestationperformsanabnormalitybased intrusion detection like statistical analysis to catch cloned keys.Furthermore, the authors do not specify how to assure malicious nodes to honestly report their keys, which is critical to the protocol effectiveness.

4. Comparative Study

Sr. no.	Reference no. Author, year	Methodology/ concept	Performance evaluation	Claims by author
1.	[8] S.Zhu, S.Setia,and S. Jajodia, 2003	LEAP: Efficient security mechanisms for large-scale distributed sensor networks	Secure, efficient in computation,communication, and storage	Key sharing approach supports in-network processing and key distribution protocol prevent node clone
2.	[9] R. Anderson, H. Chan, and A. Perrig, 2004	Key infection: Smart trust for smart dust	Prevention scheme might be useful but initial trust must be too strong to be applicable in general case	A novel way of managing keys in sensor networks, compromise nodes after their deployment
3.	[5] B. Parno, A.Perrig, V. Gligor, 2005	RM and LSMRandomized multicast scheme and line selected multicast	More secure but overhead on node	Two probabilistic detection protocols in a distributed, balanced manner to detect clone
4.	[7] Y. Zhang, W. Liu, W. Lou, and Y. Fang, 2006	Use of location-based keys to defend against node clone attack	Secure but location-based keys cannot be used in nodes at other locations, frustated	Node's private keys are bounded by both their identities and locations
5.	[11]B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy, 2007	Distributed approach called Localized Multicast	Good performance and security	Efficient distributed detection of node replication attacks in sensor networks
6.	[12] H. Choi, S. Zhu, and T. F. La Porta, 2007	SET	Increased communication burden	To detect clones by computing set operations (intersection and union) of exclusive subsets in the network
7.	[10]M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, 2007	RED and LSM protocols	Storage overhead is low and balanced, energy consumptions	Randomized, efficient, and distributed protocol for the detection of node replication attacks
8.	[14] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, 2007	Detection of clone in sensor networks using random key predistribution	Accurate detection still some problems	Keys that are present on the cloned nodes are detected by looking at how often they are used to authenticate nodes in the network.

We have done a detailed study of various approaches related to the clone attacks in WSN and identified their detectiontechniques. Then we had performed a comparative analysis on them to identify their merits and demerits. Most of the approaches overcome the security issue but they are on the cost of memory, computation, communicationoverhead.

By the above study and analysis we come to know that many of the approaches are so god still not efficient. Thus we will introduce two detection protocol,the first proposal is based on a distributed hash table (DHT), which is fully decentralized, which forms a Chord overlay network and provides the key-based routing, caching, and checking facilities for clone detection.The second protocol, named randomly directed exploration, is intended to provide highly efficient communication performance with adequate detection probability for dense sensor networks. The detection protocols is in terms of communication cost, while the detection probability is satisfactory.

5. Conclusion

Sensor nodes are subject to the node clone attack. In this paper we have reviewed different protocols and techniques for detection of clone node in WSN. By analyzing the existing system we will propose two distributed detection protocols: One is based on a distributed hash table, and the other 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 network, the randomly directed exploration presents good communication performance and minimal storage consumption for dense sensor networks.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2] D. Estrin, R. Govindan, J. S. Heidemann, and S. Kumar. "Next century challenges: Scalable coordination in

sensor networks," In Mobile Computing and Networking, 1999.

[3] Irfanullah Khan, Faheem Khan, Lala Rukh, Zaidullah and Yasir Ali, "A Survey about Security of the Wireless Sensor Network," International Journal of Computer Science and Telecommunications, Volume 3, Issue 7, July 2012.

[4] Clare, Loren P., Gregory J. Pottie, and Jonathan Agre, "Self-Organizing Distributed Sensor Networks," Proc. SPIE Aero-sense 99, 1991.

[5] B.Parno, A.Perrig andV.Gligor,"Distributed detection of node replication attacks in sensor networks," in Proc. IEEE Symp. Security Pri- vacy, pp. 49–63, 2005.

[6] H. Balakrishnan, M. F. Kaashoek, D. Karger, R. Morris, and I. Stoica, "Looking up data in P2P systems,"Commun. ACM, vol. 46, no. d2, pp. 43–48, 2003.

[7] Y.Zhang,W.Liu,W.Lou,andY.Fang,"Location-basedcompromise- tolerant security mechanisms for wireless sensor networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 247–260, Feb. 2006.

[8] S.Zhu, S.Setia,and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in Proc. 10th ACM CCS , Washington, DC, pp. 62–72, 2003.

[9] R. Anderson, H. Chan, and A. Perrig, "Key infection: Smart trust for smart dust," in Proc. 12th IEEE ICNP, pp. 206–215, 2004.

[10] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," in Proc.8th ACM MobiHoc, Montreal, QC, Canada, pp. 80–89, 2007.

[11] 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, pp. 257–267, 2007.

[12] H. Choi, S. Zhu, and T. F. La Porta, "SET: Detecting node clones in sensor networks," in Proc. 3rd SecureComm, pp. 341–350, 2007.

[13] H. Chan, A. Perrig, and D. Song," Random Key Predistribution Schemes for Sensor Networks," in IEEE SP, pp. 197–213, 2003.

[14] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," IEEE Trans. Syst.s, Man, Cybern. C, Appl. Rev., vol. 37, no. 6, pp. 1246–1258, Nov. 2007.

[15] L. Eschenauer and V. D. Gligor, "A key-management scheme for dis- tributed sensor networks," in Proc. 9th ACM Conf. Comput. Commun. Security, Washington, DC, pp. 41–47, 2002.

[16] A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc. CRYPTO, LNCS 196, pp. 47–53, 1984.

[17] R. Poovendran, C. Wang, and S. Roy, Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks. New York: Springer-Verlag, 2007.

[18] V. D. Gligor. "Security of emergent properties in ad-hoc networks," In Proceedings of International Workshop on Security Protocols, Apr. 2004.