International Journal of Advanced Computer and Mathematical Sciences
ISSN 2230-9624. Vol 3, Issue 4, 2012, pp 405-412
http://bipublication.com

AN APPROACH TO DETECT NODE CLONES IN WIRELESS SENSOR NETWORKS

Chimata Venkatarao

Dept of IT, Guru Nanak Engineering College, Hyderabad, A.P, India

[Received-11/09/2012, Accepted-02/10/2012]

ABSTRACT:

The important challenge faced by wireless sensor network security provisioning is that sensors are exposed to physical capture attacks. By distributing the clones throughout the network and starting a variety of other attacks can easily adversary launch the clone attacks by replicating the compromised node, once a sensor is compromised. Recently to address the fundamental problem, a few distributed solutions have been proposed. In this paper, for the detection of node replication attacks, we first analyze the desirable properties of a distributed mechanism. After that we show the solutions for the problem and later for detection of node replication attacks, we propose a self-healing RED protocol i.e. Randomized, Efficient, and Distributed protocol and we see that it meets the requirements. Finally it shows that our protocol is highly efficient in memory, communication and computation.

Keywords: Wireless Sensor Networks, Distributed Solutions, Physical Capture Attacks.

INTRODUCTION:

A wireless sensor network consists of spatially tribute autonomous sensors to monitor physical or environmental conditions. Wireless sensor networks can be deployed in harsh environments to fulfill both military and civil applications. A Wireless Sensor Network is a collection of sensors with limited resources that collaborate to achieve a common goal. They are often unattended and prone to different kinds of novel attacks due to their operating nature. Sensors are commonly assumed to

be not tamper-proof as an adversary could capture nodes acquiring all the information stored in the network communications. To launch a variety of malicious activities an adversary may replicate the captured sensors and deploy them in the network. This type of attack is referred as the clone attack. Since a clone has legitimate information i.e. code and cryptographic material, the same way as a non compromised node, the clone also participate in the network operations and hence clone nodes launch a variety of attacks. Some of the attacks have been described such as, by initiate a wormhole attack with a collaborating adversary, a clone could create a black hole, or inject false data or aggregate data in such a way to bias the final result. Clone attack can be characterized by two main points i.e. a clone is considered as honest to its neighbors. Honest nodes cannot be aware of the fact that they have a clone among their neighbors without global countermeasures. The adversary does not need to compromise to have a high number of nodes, indeed, the main cost of the attack has been sustained once a single node has been captured and compromised. Making further clones of the same node can be considered cheap.

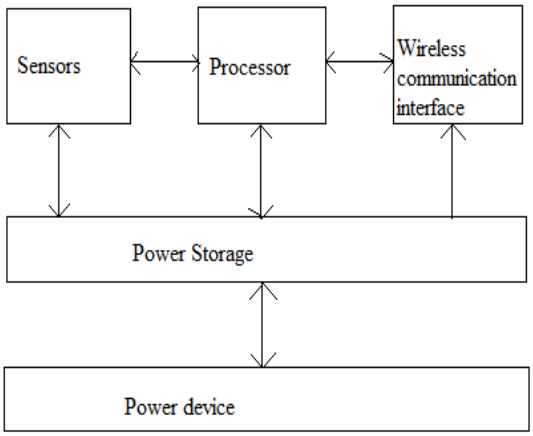

Fig Block diagram of WSN.

Only centralized or local protocols have been proposed so far to cope with the clone attack with the exception of the protocol proposed in and reviewed. Local protocols do not detect replicated nodes that are distributed in different areas of the network, while centralized protocols have a single point of failure and high communication cost. In this paper, we propose a network in which the nodes autonomously identify the presence of clones and exclude them from any further network activity i.e. self-healing mechanism. While achieving high clone detection rate continuous iteration is designed without significantly affecting the network performances. In this paper, the desirable properties of distributed mechanisms for detection of node replication attack are analyzed and show that this protocol is not completely satisfactory

with respect to the above properties. However, we propose a new randomized, efficient, and distributed (RED) protocol for the detection of node replication attacks, and we prove that our protocol meets all the above requirements. When RED and its competitor face an adversary that selectively drops messages that could lead to clone detection we further provide analytical results. Finally, the simulations of RED show that it is highly efficient as for memory; communications and computations required and show improved attack detection probability when compared to other distributed protocols.

LITERATURE REVIEW:

Centralized Base Station (BS) is the first solution for the clone attacks. Each node sends a list of its neighbors and their locations to a BS in this solution. With inconsistent locations the same node ID in two lists will result in clone detection. As the BS revokes the clones, the presence of a single point of failure (the BS) and high communication cost due to the large number of messages this solution has several drawbacks. Recently another centralized clone detection protocol has been proposed. This solution assumes that in the sensor network a random key pre distribution security scheme is implemented. A set of k symmetric keys are randomly selected from a larger pool of keys which are assigned to each node. For the detection, the keys it uses for communication by each node construct a counting Bloom filter. The BS counts the number of times each key is used in the network from all the reports. The keys used too often are considered cloned and a corresponding revocation procedure is raised. The more general problem of node compromise copes with threads of recent research. Intrusion detection system seems to require a higher overhead compared to clone detection is taken from the technique that is rooted by the approach of "misbehavior" detecting node. In particular, to recover sensor secrecy after node compromising some preliminary solutions starts appearing in the literature, but these solutions do not cope with replica attacks.

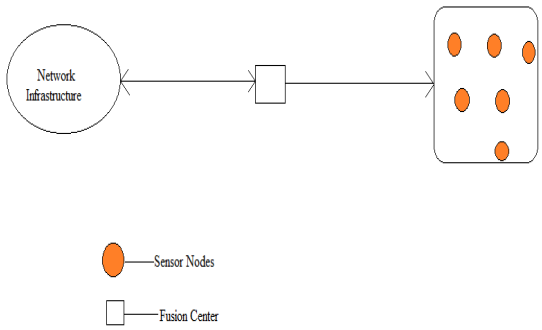

Fig Conceptual diagram of Wireless sensor network.

In particular, two distributed emergent properties have been proposed. Randomized Multicast (RM) is the first one which

distributes node location information to randomly selected nodes. To detect replicas of the network it uses the routing topology i.e. Line-Selected Multicast (LSM) which is the second one. In RM, each of its neighbors sends (with probability p) a digitally signed copy of the location claim to a set of randomly selected nodes when a node announces its location. We call witness the node that detects the existence of a node in two different locations within the same protocol run. At least one node will receive a pair of not coherent location claims if there is a replicated node and every neighbor randomly selects O (√n) destinations, with a not negligible probability. Each neighbor has to send O (√n) messages if the RM protocol implies a high communication cost.

To solve this problem, we propose the LSM protocol. The LSM protocol is similar to RM; in terms of detection probability introduces a remarkable improvement. In LSM, every neighbor first locally checks the signature of the claim, when a node announces its location and then, with probability p, forwards it to g ≥1 randomly selected destination nodes. Here the two different protocols have been proposed by the author with the aim of increasing the detection probability provided by LSM. The basic idea is to consider all the nodes within a cell as possible witnesses that are logically divided by the network into cells. Each node ID is associated with a single cell within the network is the first proposed protocol i.e. Single Deterministic Cell. The neighbors of a node a probabilistically sends 'a' to claim to a subset of the predefined witness cells for 'a' is defined in the second proposal i.e. Parallel Multiple Probabilistic Cells. A higher detection probability compared to LSM is the proposed solution. The SET protocol is the interesting distributed protocol for replicated node detection that has been recently proposed. SET leverages the knowledge of a random value broadcast by a BS to perform a detection phase. In particular, to generate independent clusters and corresponding clusters' heads the shared random value is first used. Exclusive Subset Maximal Independent Set (ESMIS) cluster heads are called Subset Leaders (SLDRs). Further, one or more trees are defined over the network graph that are generated by clusters and SLDRs within the same protocol iteration.

However, the main problem of this protocol is that it can be maliciously exploited by the adversary to revoke honest nodes and the detection protocol itself is flawed. We do not consider SET as a benchmark for our protocol due to the possibility of this attack.

Here, the authors point out the desirable properties a clone detection protocol should meet. In particular, some nodes have a higher probability to act as witnesses, so weakening the detection itself in LSM. The attacker can take control of the node with highest probability can act as witness. The simulation results show that the proposed RED protocol meets the desirable properties. In this paper, we investigate the feasibility of the RED protocol. The set of simulations presented shows that the RED protocol can be actually implemented in sensor network is analyzed. And also, as a self-healing mechanism it can be continuously iterated over the same network, without significantly affecting the detection protocol and network performance itself. We consider the influence of an attacker intervening on message routing both for RED and LSM.

THE THREAT MODEL:

Here we define a simple yet powerful adversary: It replicate one or more clones into multiple copies by compromising a certain fixed amount of nodes. In general, it is possible to cope with threat to assume that nodes are tamper-proof. Therefore, we will assume that the nodes do not have tamper-proof components consistently with a large part of the literature. However, tamper-proof hardware is expensive and energy demanding. To prevent clones from being detected by the detection protocol used in the network is the adversary goal. An adversary model is formalized by introducing the following definitions that are Definition: The distributed detection protocol by compromising a possibly small subset T of the nodes to subvert is the goal of the adversary. While M is the initial set of nodes in the network, the adversary has already compromised a set of nodes Q. For every node s, the node appeal Pwitness(s) returns the probability that s € M\Q is a witness for the next run. An adversary is characterized by two different points of view: “where” and “how” it operates. As for “where,” the adversary can be. Localized: A convex subarea is chosen by the adversary of the network and compromises sensors from that area only. Ubiquitous: The sensors choosing from the whole network is compromised by adversary. Intuitively, an adversary that needs some time to move from one point to another of the network area is described by the localized adversary, while the ubiquitous adversary, can capture nodes regardless of their position during the same time interval. As for the sequence of node capture (that is, “how”), the adversary can be: Oblivious: The next node to be

tampered with is chosen randomly among the ones that are yet to be compromised at each step of the attack sequence,

Smart: The next node to tamper with is node s, where s maximizes Pwitness(s) and s € M\Q at each step of the attack sequence. Intuitively, the oblivious adversary does not take advantage of any information about the detection protocol implemented. Conversely, to compromise the node that maximizes its appeal in order to maximize the chance that its replicas go undetected greedily chooses the smart adversary.

CONCLUSION:

In this paper, for the detection of node replication attacks, we first analyzed the desirable properties of a distributed mechanism and shown the solution and later for detection of node replication attacks, to detect node replication attacks, a self-healing, efficient, and distributed protocol are proposed. In this paper, we proposed and justified a few basic requirements an ideal protocol for distributed detection of node replicas should have based on a set model of the sensor network.

REFERENCES:

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless Sensor Networks: A Survey,” Int’l J. Computer and Telecomm. Networking, vol. 38, no. 4, pp. 393-422, 2002.

[2] R. Anderson and M.G. Kuhn, “Tamper Resistance—A Cautionary Note,” Proc. USENIX ’96 Workshop, pp. 1-11, 1996.

[3] A. Becher, Z. Benenson, and M. Dornseif, “Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks,” Proc. Int’l Conf. Security in Pervasive Computing (SPC ’06), pp. 104- 118, 2006.

[4] C. Bettstetter, “On the Minimum Node Degree and Connectivity of a Wireless Multihop Network,” Proc. MobiHoc ’02, pp. 80-91, 2002.

[5] YingpeiZeng, Jiannong Cao, Senior Member, IEEE, Shigeng Zhang, ShanqingGuo and Li Xie, "Random walk based approach to detect clone attacks in wireless sensor networks", IEEE Journal of selected areas in communication, vol 28,No. 5, June 2010.

[6] R. Brooks, P. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M.T.Kandemir, “On the Detection of Clones in Sensor Networks Using Random Key Predistribution,” IEEE Trans. Systems, Man and Cybernetics, Part C: Applications and Rev., vol. 37, no. 6, pp. 1246-1258, Nov. 2007.

[7] S. Capkun and J.-P. Hubaux, “Secure Positioning of Wireless Devices with Application to Sensor Networks,” Proc. IEEE INFOCOM ’05, pp. 1917-1928, 2005.

[8] A. Caruso, A. Urpi, S. Chessa, and S. De, “Gps-Free Coordinate Assignment and Routing in Wireless Sensor Networks,” Proc. IEEE INFOCOM ’05, pp. 150-160, 2005.

[9] H. Chan, A. Perrig, and D. Song, “Random Key Predistribution Schemes for Sensor Networks,” Proc. Symp. Security and Privacy (S&P ’03), pp. 197-213,2003.

[10] SatyajayantMisra, KabiBhattarai, and GuoliangXue, "BAMBi: Blackhole Attacks

Mitigation with Multiple Base Stations in Wireless Sensor Networks", IEEE ICC 2011 proceedings.

[11] H. Choi, S. Zhu, and T.F. La Porta, "SET: Detecting Node Clones in Sensor Networks," Proc. Int'l Conf. Security and Privacy in Comm. Networks and the Workshops (SecureComm '07), pp. 341-350, 2007.

[12] C. Cocks, "An Identity Based Encryption cheme Based on Quadratic Residues," Proc. IMA Int'l Conf. '01, pp. 360-363, 2001.

[13] M. Conti, R. Di Pietro, A. Gabrielli, L.V. Mancini, and A. Mei, "The Quest for Mobility Models to Analyse Security in Mobile Ad Hoc Networks ,"Proc. Seventh Int'l Conf. Wired/Wireless Internet Comm. (WWIC '09), pp. 85-96, 2009.

[14] M. Conti, R. Di Pietro, and L.V. Mancini, "Secure Cooperative Channel Establishment in Wireless Sensor Networks," Proc. IEEE Pervasive Computing and Comm. (PERCOM '06) Workshop, pp. 327- 331, 2006.

[15] M. Conti, R. Di Pietro, and L.V. Mancini, "ECCE: Enhanced Cooperative Channel Establishment for Secure Pair-Wise Communication in Wireless Sensor Networks," Ad Hoc Networks, vol. 5, no. 1, pp. 49-62, 2007.

[16] M. Conti, R. Di Pietro, L.V. Mancini, and A. ei, "Mobility and Cooperation to Thwart Node Capture Attacks in Manets," J. Wireless Comm. And Networking. Feb. 2009.

[17] M. Conti, R. Di Pietro, L.V. Mancini, and A. ei, "Requirements and Open Issues in Distributed Detection of Node Identity Replicas in WSN," Proc. IEEE Int'l Conf. Systems, Man and Cybernetics (SMC '06), pp. 1468-1473, 2006.

[18] M. Conti, R. Di Pietro, L.V. Mancini, and A. Mei, "A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks," Proc. MobiHoc '07, pp. 80-89, 2007.

[19] M. Conti, R. Di Pietro, L.V. Mancini, and A. ei, "Emergent Properties: Detection of the Node-Capture Attack in Mobile Wireless Sensor Networks," Proc. ACM Conf. Wireless Network Security (WiSec '08), pp. 214-219, 2008.

[20] B. Deb, S. Bhatnagar, and B. Nath, "ReInForM: Reliable Information Forwarding Using Multiple Paths in Sensor Networks," Proc. IEEE Int'l Conf. Local Computer Networks (LCN '03), pp. 406-415, 2003.

[21] M. Demirbas and Y. Song, "An RSSI-Based Scheme for Sybil Attack Detection in Wireless Sensor Networks," Proc. Int'l Symp. World of Wireless, Mobile and Multimedia Networks (WOWMOM '06), pp. 564-570, 2006.

[22] A. Derhab and N. Badache, "A Self-Stabilizing Leader Election Algorithm in Highly Dynamic Ad Hoc Mobile Networks," IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 7, pp. 926-939, July 2008.

[23] R. Di Pietro, D. Ma, C. Soriente, and G. Tsudik, "Posh: Proactive Co-Operative Self-Healing in Unattended Wireless Sensor Networks," Proc. IEEE Symp. Reliable Distributed Systems (SRDS), pp. 185- 194, 2008. [24] R. Di Pietro and L.V. Mancini, "Intrusion Detection Systems," Advances in Information Security, vol. 38, Springer, 2008.

[25] R. Di Pietro, L.V. Mancini, and A. Mei, "Energy Efficient Node-to-Node Authentication and Communication Confidentiality in Wireless Sensor Networks," Wireless Networks, vol. 12, no. 6, pp. 709-721, 2006.

[26] R. Di Pietro, L.V. Mancini, A. Mei, A. anconesi, and J. Radhakrishnan, "Connectivity Properties of Secure Wireless Sensor Networks," Proc. Workshop

Security of Ad Hoc and Sensor Networks (SASN ’04), pp. 53-58, 2004.

[27] R. Di Pietro, L.V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, “Sensor Networks That Are Provably Resilient,” Proc. Int’l Conf. Security and Privacy in Comm. Networks and the Workshops (SecureComm ’06), pp. 1-10, 2006.

[28] R. Di Pietro, L.V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, “Playing Hide-and-Seek with a Focused Mobile Adversary in Unattended Wireless Sensor Networks,” Ad Hoc Networks, vol. 7,no. 8, pp. 1463-1475, 2009.

[29] J.R. Douceur, “The Sybil Attack,” Proc. Int’l Workshop Peer-to-Peer Systems (IPTPS ’01), pp. 251- 260, 2002.

[30] D. Dubhashi, O. Ha¨ggstro¨m, L. Orecchia, A. Panconesi, C. Petrioli, and A. Vitaletti, “Localized Techniques for Broadcasting in Wireless Sensor Networks,” Algorithmica, vol. 49, no. 4, pp. 412-446, 2007.

[31] J. Elson and D. Estrin, “Time Synchronization for Wireless Sensor Networks,” Proc. Int’l Parallel

[32] J. Elson, L. Girod, and D. Estrin, “Fine-Grained Network Time Synchronization Using Reference Broadcasts,” SIGOPS Operating Systems Rev., vol. 36, pp. 147-163, 2002.

[33] L. Eschenauer and V.D. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” Proc. Conf. Computer and Comm. Security (CCS ’02), pp. 41-47, 2002.

[34] F. Fu, J. Liu, and X. Yin, “Space-Time Related Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks,” Proc. Int’l Conf. Wireless Comm., Networking and Mobile Computing (WiCom ’07), pp. 2692-2696, 2007.

[35] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, “Highly-Resilient, Energy-Efficient Multipath Routing in Wireless Sensor Networks,” SIGMOBILE Mobile Computing and Comm. Rev., vol. 5, no. 4, pp. 11-25, 2001.

[36] V.D. Gligor, “Emergent Properties in Ad-Hoc Networks: A Security Perspective,” Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS ’06), p. 1, 2006.

[37] Y.C. Hu, A. Perrig, and D.B. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks,” Proc. IEEE INFOCOM ’03, pp. 1976-1986, 2003.

[38] C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” Ad Hoc Networks, vol. 1, nos. 2/3, pp. 293-315, 2003.

[39] B. Karp and H.T. Kung, “GPSR: Greedy Perimeter Stateless Routing for Wireless Networks,” Proc. ACM MobiCom ’00, pp. 243- 254, 2000.

[40] J. Kong, H. Luo, K. Xu, D.L. Gu, M. Gerla, and S. Lu, “Adaptive Security for Multi-Layer Ad-Hoc Networks,” Wireless Communication and Mobile Computing, vol. 2, no. 5, pp. 533-547, Wiley Inter science Press, 2002.

[41] S. Kwon and N.B. Shroff, “Paradox of Shortest Path Routing for Large Multi-Hop Wireless Networks,” Proc. IEEE INFOCOM ’07, pp. 1001-1009, 2007.

[42] A. Mei and J. Stefa, “Routing in Outer Space: Fair Traffic Load in Multi-Hop Wireless Networks,” Proc. MobiHoc ’08, pp. 23-32, 2008.

[43] J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil Attack in Sensor Networks: Analysis & Defenses,” Proc. Int’l Symp. Information Processing in Sensor Networks (IPSN ’04), pp. 259-268, 2004.