International Journal of Science Engineering and Advance Technology

A New Approach for Node Replica Detection in WSN

1 **Sri. M. Vamsi Krishna,** 2**T. Ravi Kumar**
1,2 Dept. of CSE, Chaitanya Institute of Science &Technology, Kakinada, AP, India

Abstract:
Wireless sensor networks are a collection of sensor nodes scattered over the area for data collection. But the main problem is it is in danger to the node clone. To identify Node clone proposing distributed hash table which a fully decentralized, key-based caching and checking system .next introducing distributed detection protocol provides good communication performance for large sensor networks. sensor-MAC a new MAC protocol explicitly designed for wireless sensor networks for reducing energy consumption. Our protocol also has good scalability and collision avoidance capability.

1. Introduction

A Wireless Sensor Network is a group of specialized transducers with a communications infrastructure intended to monitor and record conditions at locations. A sensor network consists of multiple detection stations called sensor nodes; the transducer generates electrical signals based on sensed physical effects and phenomena. The transceiver, which can be hard-wired or wireless, receives commands from a central computer and transmits data to that computer.

The main problems deals with WSN are easy to hack, low speed of communication, high cost and interference. Because of this hackers many attacks affects the WSN. Among those attacks serious and dangerous one is *node clone attack*. In this attack the adversary may capture some nodes in the network when they are in hostile environment and extract the secret credentials data and information from nodes, reprograms or modifies the data and creates replicas or clones of such nodes in the network. Then these compromised nodes plays active in network and thus the adversary may gain the control over the network. Thus security of network had lost and more over these cloned nodes can create more attacks like DOS inside the network which corrupts the information. If these clones are left undetected, the network is unshielded to attackers and thus extremely vulnerable. Therefore in this paper, an effective two novel node clone detection protocols are proposed to detect the node clones. The previous works incurs more communication cost and required to transmit more messages resulted in the reduction of life time. The first one is *distributed hash table* (DHT) which is based on hash table value of (key, record) by which a fully decentralized, key-based caching and checking system is constructed to catch nodes. DHT enables sensor nodes to construct the over lay network. The key plays vital role in DHT mechanism which determines the destination node of the message. But this DHT incurs same communication cost as previous, have some storage consumption and strong detection probability. Second one is distributed detection protocol, named *randomly directed exploration (RDE)* in which probabilistic directed forwarding technique along with random initial direction and border determination. Every node contains signed version of neighbor list and the detection round is initiated by sending claiming message by the nodes to randomly selected neighbors. The communication cost is reduced by using border determination. And this protocol has to store only the list of neighbor nodes so consumes less memory. So the RDE stands with low communication cost, less storage consumption and high detection probability. The RDE and DHT protocols are only used to detect the node clones in the WNS.

2. Related Work:

The Sybil attack is related to the node replication attack in the Sybil attack, a malicious node gains an unfair advantage by claiming multiple identities. Douceur presents counter measures for peer-to-peer networks that involve resource verification (computation, communication, and memory). Newsome et al. present techniques to defend against the Sybil attack in sensor networks. Their countermeasures include wireless network testing, key space verification, and central node registration. Only their centralized node registration technique can detect a node replication attack, but it is brittle in the face of node compromise and has a high overhead, as we show in this paper. Bawa et al. propose an algorithm for counting the number of members of a peer-to-peer network that is related in spirit to our approach; they propose a random sampling approach that provides an estimate of the network size after $O(\sqrt{n})$ samples are drawn and a duplicate node is sampled (for a network of size n), by using the birthday paradox. Our Randomized Multicast also relays on the birthday paradox.

Literature Survey:

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, we propose two new algorithms based on emergent properties. 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.

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, we propose two new algorithms based on emergent properties 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. We show that 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.

3. Problem Statement:

3.1: Existing System

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.

Disadvantages :

- Communication cost is high.
- Memory consumption is also high.
- It consumes more energy for clone node detection
- Detection accuracy is also low.

3.2: Proposed System

- In this project, we present two novel, practical node clone detection protocols with different tradeoffs on network conditions and performance. The first proposal is based on a distributed hash table by which a fully decentralized, key-based caching and checking system is constructed to catch cloned nodes.

- Introducing new MAC Protocol along with distributed hash table which reduces energy consumption of sensors.

- **Advantages:**

- The DHT-based protocol can detect node clone with high security level and holds strong resistance against adversary's attacks.

- Our protocol also has good scalability and collision avoidance capability. It achieves good scalability and collision avoidance by utilizing a combined scheduling and contention scheme.

Algorithme

Algorithm 1:

dht_ handle message(Mα4β) handle a message in the DHT-based detection, where y is the current node's Chord coordinate, finger[i] is the first node on the ring that succeeds key((y+2b-I mod 2b),I £ [1,t] ,successors [j] is the next jth successor j £[1,g][1].

Output: NIL if the message arrives at its destination; otherwise it is the ID of the next node that receives the message in th Chord overlay network[1].
1: key<—11 (seed||id_β)
2: **if** key £ [predecessor] **then** {has reached destination}
3: inspect $M_{\alpha 4\beta}$ {act as an inspector, see Algorithm 2}
4: **return** NIL
5: for i=1 to g **do**
6: **if** key £(y, successors [i]) **then** {destination is in the nex Chord hop}
7: inspect $M_{\alpha 4\beta}$ {act as an inspector, see Algorithm 2}
8: **return** successors [i]
9: **for** j= 1 to t **do** {for normal DHT routing process}
10: **if** key £ [$(y+2^{b-1} \bmod 2^b, y)$], **then**
11: **return** finger [j]
12: **return** successor [g]

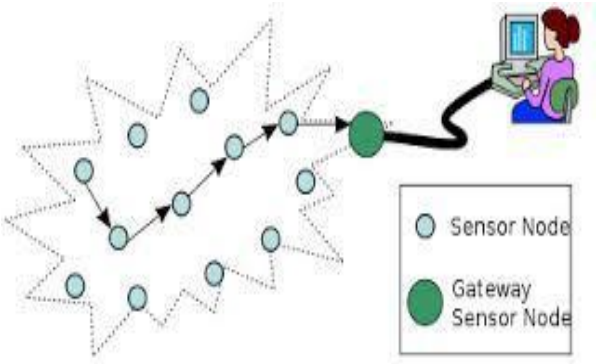
Algorithm 2: inspect $M_{\alpha 4\beta}$: Inspect a message to check for clon detection in the DHT-based detection protocol
1: verify the signature of $M_{\alpha 4\beta}$
2: if id_β found in cache table **then**
3: if id_β has two distinct locations {found clone, become witness}
4: broadcast the evidence
5: **else**
6: buffer $M_{\alpha 4\beta}$ into cache table

S-Mac Protocol

1. The node first listens for a certain amount of time. If it does not hear a schedule from another node, it randomly chooses a time to go to sleep and immediately broadcasts its schedule in a SYNC message, indicating that it will go to sleep after t seconds. We call such a node a *synchronizer*, since it chooses its schedule independently and other nodes will synchronize with it.
2. If the node receives a schedule from a neighbor before choosing its own schedule, it follows that schedule by setting its schedule to be the same. We call such a node a *follower*. It then waits for a random delay td and rebroadcasts this schedule, indicating that it will sleep in T-TD seconds. The random delay is for collision avoidance, so that multiple followers triggered from the same synchronizer do not systematically collide when rebroadcasting the schedule.

3. If a node receives a different schedule after it selects and broadcasts its own schedule, it adopts both. It broadcasts its own schedule before going to sleep.

4. System Architecture:



5. Modules:

Modules Description:

Setting up Network Model:

Our first module is setting up the network model. We consider a large-scale, homogeneous sensor network consisting of resource-constrained sensor nodes. Prior to deployment, each legitimate node is allocated a unique ID and a corresponding private key by a trusted third party.

Initialization Process:

To activate all nodes starting a new round of node clone detection, the initiator uses a broadcast authentication scheme to release an action message including a monotonously increasing nonce, a random round seed, and an action time. The nonce is intended to prevent adversaries from launching a DoS attack by repeating broadcasting action messages.

Claiming neighbor's information:

Upon receiving an action message, a node verifies if the message nonce is greater than last nonce and if the message signature is valid. If both pass, the node updates the nonce and stores the seed. At the designated action time, the node operates as an observer that generates a claiming message for each neighbor (examinee) and transmits the message through the overlay network with respect to the claiming probability.

Processing claiming messages:

A claiming message will be forwarded to its destination node via several Chord intermediate nodes. Only those nodes in the overlay network layer (i.e., the source node, Chord intermediate nodes, and the destination node) need to process a message, whereas other nodes along the path simply route the message to temporary targets.

Sink Module:

The sink receives data from sensors of the sensor network. Each time the sink receives a query from a user. Which process the queries based on their data and return the query results to the sink.

Performance Analysis:

- For the DHT-based detection protocol, we use the following specific measurements to evaluate its performance:

• Average number of transmitted messages, representing the protocol's communication cost;

• Average size of node cache tables, standing for the protocol's storage consumption;

8. Conclusion:

Sensor nodes lack tamper-resistant hardware and are subject to the node clone attack. In this paper, we present two distributed detection protocols: 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, 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 networks by one deterministic witness and additional memory-efficient, probabilistic witnesses, the randomly directed exploration presents outstanding communication performance and minimal storage consumption for dense sensor networks.

9. 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, andY. Fang, "Location-based compromisetolerant 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 key predistribution," *IEEE Trans. Syst.s, Man, Cybern. C, Appl. Rev.*, vol. 37, no. 6, pp. 1246–1258, Nov. 2007.
[10] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. 9th ACM Conf. Comput. Commun. Security*, Washington, DC, 2002, pp. 41–47.

Authors:

Sri.M.Vamsi krishna, well known Author and excellent teacher Received M.Tech (AI &R), M.Tech (CS) from Andhra University is working as Professor and HOD, Department of CSE, Chaitanya Institute Science and Technology. He has 13 years of teaching & research experience. He has 20 publications of both national and international conferences /journals. His area of Interest includes AI, Computer Networks, information security, flavors of Unix Operating systems and other advances in computer Applications..

Mr T. Ravi Kumar is a student of Chaitanya Institute Science of Technology, MadhavaPatnam, Kakinada. He received his B.Tech in Electronics & Communication Engineering from Kakatiya University, Warangal. Presently he is pursuing his M.Tech (Computer Science & Engineering) from this college. His area of interest includes Computer Networks,. ERP Systems and Object oriented Programming languages, all current trends and techniques in Computer Science.