CLONE DETECTION

N.Supriya, D.BullaRao***

**M.Tech Student Computer Science Engineering, SITS, JNTU-A, Tirupathi, AP*

***Assistant Professor, Dept. of CSE, SITS, JNTU-A, Tirupathi, AP*

Abstract The wide Open Nature of WSN is a medium that leaves an intentional Inner and outer interference attacks on Wireless Devices, typically referred to as Clone Attacks. As the wireless networks are defenseless to the node clone and having more distributed protocols for detecting attacks. We require a strong assumptions and practical large scale protocol for sensor networks to provide protection to the network data transmission. In the proposed research we discuss two new frame works for node clone detection protocols with various tradeoffs on the wireless network conditions and performance. The first activity is based on distributed has table in which a fully decentralized key based checking and caching organism is developed to catch cloned nodes effectively. Here the protocol performance provides efficient storage consumption and high security level through probability model and resulting equations with necessary adjustments for applications in real. The simulation takes the data of various applications in real and communicates through DHT protocol for showing efficient result rather than old protocols. The DHT protocols gains similar communication cost as old approaches and considers a little bit higher for selected scenarios. The second protocol called distributed detection protocol or also named as randomly directed exploration protocol provides a good communication performance for solid sensor networks through a probabilistic directed forwarding technique. This also uses random initial direction and border determination. The proposed simulation result upholds the protocol design and shows a efficient communication overhead and satisfactory detection probability.

Index Terms— Information retrieval, spatial index, keyword search.

I. INTRODUCTION

Wireless Sensor Network (WSN) is a group of wireless sensor nodes that have small capacities of sensing, processing which are deployed over a geographical area for sensing physical phenomenon. Usually, these sensor nodes send their sensed data to a base station for further processing. They are prepared with low cost small capacity batteries which are, non-rechargeable and irreplaceable. Hence,

network lifetime is considered as an important issue for many applications.

The WSN is built of "nodes" from a few to more than hundreds, where each node is connected to several sensors. Every sensor network node are having several parts: a radio transceiver with an internal antenna or connection that have outside 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 that have capacity that is having a shoebox down to the size of a grain of dust, even though functioning "motes" of actual microscopic dimensions that should be created. The cost of sensor nodes is equally changeable, depending on the complexity of the each sensor nodes. Sensor nodes result in corresponding on resources such as energy, memory, computational speed and communications bandwidth that constraints size and cost. 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.

In the proposed research we discuss two new frame works for node clone detection protocols with various tradeoffs on the wireless network conditions and performance. The first activity is based on distributed has table in which a fully decentralized key based checking and caching organism is developed to catch cloned nodes effectively. Here the protocol performance provides efficient storage consumption and high security level through probability model and resulting equations with necessary adjustments for applications in real. The simulation takes the data of various applications in real and communicates through DHT protocol for showing efficient result rather than old protocols. The DHT protocols gains similar communication cost as old approaches and considers a little bit higher for selected scenarios. The second protocol called distributed detection protocol or also named as randomly directed exploration protocol provides a good communication performance for solid sensor networks through a probabilistic directed forwarding technique. This also uses random initial direction and border determination. The proposed simulation result upholds the protocol design and shows a efficient communication overhead and satisfactory detection probability.

II. BRIEF INFORMATION ABOUT THE AREA OF PROJECT

Modern IP network services provide for the simultaneous digital transmission of voice, video, and data. These services require

congestion control protocols and algorithms which can solve the packet loss parameter can be kept under control. Congestion control is therefore, the cornerstone of packet switching networks. It should prevent congestion collapse, provide fairness to competing flows and optimize transport performance indexes such as throughput, delay and loss. The literature abounds in papers on this subject; there are papers on high-level models of the flow of packets through the network, and on specific network architecture.

In this project, we consider and design an advanced protocol for a sophisticated adversary model in which we execute a new set of rules for better and safer infrastructure network protocols. To address the problem of jamming under an exterior threat model between a variety of nodes of wireless in the paper also focuses on a algorithm called elliptic. The probable complicated competitor who is aware of network secrets and the completing details of network protocols at any layer in the network stack.

The projected source code is to send the data to the target through a Inter leaver, Channel Encoder and the Modulator. For a model we be going to a imitation of declaration in wireless sensor networks. The node is able to send messages to client nodes based on the port number and the protected encrypted declaration is routed through one of the servers which are centralized and used for program. Here surfer is able to select a file or series of files by clicking browse button.

The messages is separated into packets and broken packets with length 48 bytes are encrypted into protected scheme using a lot of methods designed in the project initiate by user in order to send messages , we suggest cryptography encryption, elliptic encryption, strong and puzzle methods based on customer selection. The cipher text now uses Acknowledgement improvement between the nodes to rise above the jamming activity.

III. PROBLEM DEFINITION

In general, wireless sensor networks consist of hundreds and thousands of low-cost, resource-constrained, circulated sensor nodes, that was scatter in the surveillance area randomly that working without attendance. WIRELESS sensor networks (WSNs) have a great deal of attention to gain in the past decade due to their large series of application areas and formidable design challenges. The operation environment is hostile, security mechanisms against adversaries taken into consideration.

The node clone is a serious and dangerous more than physical attacks to sensor networks. The production expense limitation, sensor nodes are generally short of tamper-resistance hardware components; than adversary can capture a few nodes, extract code and all secret credentials, those materials to clone a lot of nodes sensor hardware. Those cloned nodes that legitimate seems freely join the sensor network that significantly enlarge the adversary's capacities to manipulate the network maliciously

DISADVANTAGES OF EXISTING SYSTEM:

- There are many physical attacks to sensor networks, the node clone is a dangerous.
- Storage consumption performance was insufficient for existing system and low security level.
- Among many physical attacks to sensor networks, the node clone is a serious and dangerous one.
- Insufficient storage consumption performance in the existing system and low security level.

IV. LITERATURE SURVEY

1) Distributed detection of node replication attacks in sensor networks

AUTHORS: B. Parno, A. Perrig, and V. Gligor

The low-cost, off-the-shelf hardware components in unshielded sensor-network nodes leave them exposed to compromise. With little effort, an adversary may capture nodes, analyze and replicate them, and secretly insert these replicas at planned locations within the network. Such attacks have severe consequences that allow the adversary to disconnect significant parts of the network. Earlier node replication recognition schemes depend primarily on centralized mechanisms with each points of failure on neighborhood voting protocols that fail to detect spread replications. To address these original limitations. We propose the new two algorithms 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 supply globally-aware, spread node-replica detection, and line-selected multicast displays particularly strong presentation characteristics. We show that evolving algorithms represent a promising new move towards the sensor network security;

moreover, our results naturally extend to other networks in which nodes can be captured, replicated by an adversary.

2) Looking up data in P2P systems

AUTHORS: H. Balakrishnan, M. F. Kaashoek, D. Karger, R. Morris, and I. Stoica

The main challenge in P2P computing is to design and execute a robust and scalable circulated system composed of inexpensive. Individually unreliable computers in unrelated administrative domains. The participants in a classic P2P system might include computers at homes, schools, and businesses grow to more than a few million simultaneous participants.

3) Location-based compromise tolerant security mechanisms for wireless sensor networks

AUTHORS: Y. Zhang,W. Liu,W. Lou, andY. Fang

Node compromise is a serious threat to wireless sensor networks deployed in unattended and hostile environments. To moderate the contact of compromised nodes that 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 entity 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 locality. We also present proficient approaches to establish a shared key between any two network nodes. In contrast to previous key concern solutions, our approaches feature nearly ideal resilience to node compromise low communication and overhead, low memory necessities and high network scalability. We demonstrate the efficacy of LBKs in counteracting several notorious attacks against sensor networks such as the Sybil attack, the individuality replication attack, wormhole and sinkhole attacks. Finally, we propose a location-based threshold-endorsement scheme, called LTE 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) LEAP: Efficient security mechanisms for large-scale distributed sensor networks

AUTHORS: S. Zhu, S. Setia, and S. Jajodia

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

inspection that a typical type of messages exchanged among sensor nodes have different security necessities that a single keying mechanism is not suitable for meeting these unlike security requirements. 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 the nodes in the network. The protocol used for updating these keys.

5) Key infection: Smart trust for smart dust

AUTHORS: R. Anderson, H. Chan, and A. Perrig

Future distributed systems may include large self-organizing networks of near by communicating sensor nodes any small number which may be subtended by an adversary. Provided that security for these sensor networks is important but the problem is complicated by the fact that managing cryptographic key material is hard: low-cost nodes are neither tamper-proof nor capable of performing public key cryptography efficiently. the key distribution problem can be dealt that show how within environments with a in some extent, passive adversary: a node wishing to correspond securely with other nodes simply generates a symmetric key and sends it in the clear to its neighbours. Despite the apparent insecurity of this primitive, we can use mechanisms for key updating, multipath secrecy amplification and multihop key spread to build up particularly resilient trust networks that are most a fixed section of communications links can be eavesdropped. We discuss applications in which this statement is reasonable. Many systems must perforce cope with principals who are authenticated weakly; the resulting issues have often been left in the 'too hard' tray. One particular interest of sensor networks is that they present a adequately compact and obedient version of this problem. We can perform quantitative analyses and simulations of substitute strategies, some of which we nearby here. We also hope that work may start to challenge the common belief that verification is considerably about bootstrapping trust. We argue that, in circulated systems where the opponent can challenge any small quantity of nodes.

V. COMPARITIVE STUDY

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. Analogous to previous distributed detection approaches;

we assume that an identity-based public-key cryptography facility is available in the sensor network. Prior to deployment, each legitimate node is allocated a unique ID and a corresponding private key by a trusted third party. The public key of a node is its ID, which is the essence of an identity-based cryptosystem. Consequently, no node can lie to others about its identity. Moreover, anyone is able to verify messages signed by a node using the identity-based key.The source nodes in our problem formulation serve as storage points which cache the data gathered by other nodes and periodically transmit to the sink, in response to user queries. Such network architecture is consistent with the design of storage centric sensor networks

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. Nodes can start transmitting claiming messages at the same time, but then huge traffic may cause serious interference and degrade the network capacity. To relieve this problem, we may specify a sending period, during which nodes randomly pick up a transmission time for every claiming message.

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. Algorithm 1 for handling a message is the kernel of our DHT-based detection protocol. If the algorithm returns NIL, then the message has arrived at its destination. Otherwise, the message will be subsequently forwarded to the next node with the ID that is returned.

Sink Module:

The sink is the point of contact for users of the sensor network. Each time the sink receives a question from a user, it first translates the question into multiple queries and then disseminates the queries to the corresponding mobile relay, which process the queries based on their data and return the query results to the sink. The sink unifies the query results from multiple storage nodes into the final answer and sends it back to the user.

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;

• Average number of witnesses, serving as the protocol's security level because the detection protocol is deterministic and symmetric.

VI . CONCLUSION

The clone attack process provides lack of tamper resistant for hardware and software which subjected to clone attack process. In this research we have presented two distributed clone detection protocols. The first protocol is based on distributed hash table which provides a chord overlay networks and based on the routing, caching and checking facilities for clone detection with other users and probabilistic technique with directed activity to achieve fast and efficient communication overhead for good and satisfactory clone detection probability. With the proposed DHT protocol provides high security level for all kinds of sensor networks by one or more deterministic observers and additional efficient memory handling with probabilistic observers with randomly directed exploration presents outstanding communication performance with minimal storage and consumption for dense sensor networks.

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 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 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.

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

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

[13] 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.

[14] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Schenker, "A scalable content-addressable network," in *Proc. SIGCOMM*, San Diego, CA, 2001, pp. 161–172.

[15] I. Stoica, R.Morris, D. Liben-Nowell, D. R. Karger,M. F.Kaashoek, F. Dabek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup protocol for internet applications," *IEEE/ACM Trans. Netw.*, vol. 11, no. 1, pp. 17–32, Feb. 2003.

[16] A. I. T. Rowstron and P. Druschel, "Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems," in *Proc. IFIP/ACM Int. Conf. Distrib. Syst. Platforms Heidelberg*, 2001, pp. 329–350.

[17] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in *Proc. 1st Int. Conf. Simulation Tools Tech. Commun., Netw. Syst. Workshops*, Marseille, France, 2008, pp. 1–10.

[18] A. Awad, C. Sommer, R. German, and F. Dressler, "Virtual cord protocol (VCP): A flexible DHT-like routing service for sensor networks," in *Proc. 5th IEEE MASS*, 2008, pp. 133–142.

[19] R. Diestel, *Graph Theory*, 3rd ed. New York: Springer, 2006.

BIOGRAPHY

Author:

N.Supriya, M.Tech Swetha Institute of Technology And Science, jntu-a,ap, Areas of interest:Networking

Email: supriyakumaraug14@gmail.com

Guide:

D.BullaRao, Assistant Professor, Dept. of CSE, SITS, jntu-A, Tirupathi, AP,

Email: bullaraodomathoti @gmail.com