A CLONE NODE DETECTION SYSTEM USING CLOCK SYNCHRONIZATION AND POSITION EVALUATION

M. Jayapriya [1], B. Rosiline Jeetha[2]

ABSTRACT

Due to the high mobility and infrastructure free environment MANET suffers from plenty of security threads. The proposed system deals with the problem of mobile clone attack, which also known as spoofing attack. The attacker may use the mobile node id and other details and can create duplicated nodes in the network. Those clone nodes can be used for data stealing and other misbehaving activities. The proposed system addresses the node cloning attack in MANETs. This has been implemented from the perception that mobility, synchronization, fast and cost effective. The aim of this system is providing a new mechanism which is named as CCCD (**C**ustomized **C**lock based **C**lone **D**etection) protocol, which helps to computing effectively and with limited resource usage network global security properties. The proposed system utilizes Port hopping method for different clock timings. Based on the clock settings the mobile node will transmit the time and location stamp to the control units. The experiment and simulation results show the performance of the proposed protocol CCPH with FCD algorithm earns better results than the existing system.

Index Terms – Distributed detection, Distributed hash table, node clone attack, randomly directed exploration, Wireless Sensor Networks (WSNs).

I. ABOUT MANET

MOBILE ad hoc networks (MANETs) have expanded a great deal of concentration since of its considerable advantages brought about by multichip, infrastructure-less transmission. Due to the error prone wireless channel and the dynamic network topology, reliable data delivery in MANETs, especially in challenged environments with high mobility remains an issue. Oftentimes these services are required over highly dynamic networks, such as mobile ad hoc, vehicular, or wireless sensor networks (WSNs). These networks are dynamic due to the mobility of the nodes in the network and/or the random sleep/awake cycles that are often utilized to minimize energy dissipation of the devices. Providing robust data sharing and routing in such dynamic network environments is an important design challenge for supporting these applications. In some wireless applications, the source and intermediate nodes are mobile, but the intruders effectively corrupt the contents in this thesis, in order to support any type of clone detection service to particular devices, the source nodes and route node must know the locations of the intruders. This can be provided by a service discovery protocol that sits outside the routing protocol, updating the source with the current location of the sink nodes. In either case, the routing protocol can assume knowledge

[1]Research Scholar, Rvs College Of Arts And Science, Sulur, Coimbatore - 641 002. E-mail id: jesinpriya@gmail.com

[2]Assistant Professor, Rvs College Of Arts And Science, Sulur, Coimbatore - 641 002. E-mail id: roseline@rvsgroup.com

of the sinks' locations. We can exploit this knowledge to design a stateless multicast routing protocol.

The proposed system effectively identify the clone nodes with customized clocks, user can set their time details efficiently , inter cluster and selfish node identification is too difficult, modern world process are done scheme,

1.1 Introduction To Mobile Adhoc Network

The field of wireless and mobile communications has experienced an unprecedented growth during the past decade. Current second-generation (2G) cellular systems have reached a high penetration rate, enabling worldwide mobile connectivity. Mobile users can use their cellular phone to check their email and browse the Internet. Recently, an increasing number of wireless local area network (LAN) hot spots is emerging, allowing travelers with portable computers to surf the Internet from airports, railways, hotels and other public locations. Broadband Internet access is driving wireless LAN solutions in the home for sharing access between computers. In the meantime, 2G cellular networks are evolving to 3G, offering higher data rates, infotainment and location-based or personalized services. However, all these networks are conventional wireless networks, conventional in the sense that as prerequisites, a fixed network infrastructure with centralized administration is required for their operation, potentially consuming a lot of time and money for set-up and maintenance.

Furthermore, an increasing number of devices such as laptops, personal digital assistants (PDAs), pocket PCs, tablet PCs, smart phones, MP3 players, digital cameras, etc. are provided with short-range wireless interfaces. In addition, these devices are getting smaller, cheaper, more user friendly and more powerful. This evolution is driving a new alternative way for mobile communication, in which mobile devices form a self creating, self-organizing and self-administering wireless network, called a *mobile ad hoc network*. This paper discusses the characteristics, possible applications and network layer challenges of this promising type of network.

1.2 MANET Applications

With the increase of portable devices as well as progress in wireless communication, ad-hoc networking is gaining importance with the increasing number of widespread applications. Ad-hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. The set of applications for MANET is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infra structured environment into the ad hoc context, a great deal of new services can and will be generated for the new environment.

1.2.1 Military Battlefield:

Military equipment now routinely contains some sort of computer equipment. Ad- hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of ad hoc network came from this field.

1.2.2 Commercial Sector:

Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small hand held. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

1.2.3 Local Level:

Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft, mobile ad hoc communications will have many applications.

1.2.4 Personal Area Network (PAN):

Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone). Tedious wired cables are replaced with wireless connections. Such an ad hoc network can also extend the access to the Internet or other networks by mechanisms e.g. Wireless LAN (WLAN), GPRS, and UMTS. The PAN is potentially a promising application field of MANET in the future pervasive computing context.

1.2.5 MANET-VoVoN:

A MANET enabled version of JXTA peer-to-peer, modular, open platform is used to support user location and audio streaming over the JXTA virtual overlay network. Using MANET-JXTA, a client can search asynchronously for a user and a call setup until a path is available to reach the user. The application uses a private signaling protocol based on the exchange of XML messages over MANET-JXTA communication channels.

II. Related Work

Cloning attacks can further facilitate a variety of traffic injection attacks [1], [2], such as attacks on access control lists, rogue access point (AP) attacks, and eventually Denial of Service (DOS) attacks. A broad survey of possible cloning attacks can be found in [3], [4]. Moreover, in a large-scale network, multiple adversaries may masquerade as the same identity and collaborate to launch malicious attacks such as network resource utilization attack and denial-of-service attack quickly. Therefore, it is important to

1) Detect the presence of cloning attacks, 2) determine the number of attackers, and 3) localize multiple adversaries and eliminate them.

The traditional approach to prevent cloning attacks is to use cryptographic-based authentication [5], [6], [7]. I have introduced a secure and efficient key management (SEKM) framework. SEKM builds a Public Key Infrastructure (PKI) by applying a secret sharing scheme and an underlying multicast server group. Wool [6] implemented a key management mechanism with periodic key refresh and host revocation to prevent the compromise of authentication keys. An authentication framework for hierarchical, ad hoc

sensor networks is proposed in [7]. However, the cryptographic authentication may not be always applicable because of the limited resources on wireless devices and lacking of a fixed key management infrastructure in the wireless network.

To detect a node cloning attack, the author of [8] proposed a location information-based detection method by using cryptography with a GPS and a time stamp. This approach requires each node to advertise its position obtained by the GPS and the time stamp to enable each node to obtain the location information of the other nodes. This approach detects the node cloning by calculating the distance between two nodes that claim to be neighbors and checking the likelihood that the link is based on a maximum transmission range. The main drawback of this approach is that it might not work in a situation where all MANET nodes are not equipped with a GPS. Furthermore, attackers can still advertise false information and make it hard for other nodes to detect the attack. Through simulations, the authors show that node cloning can have a devastating impact on the target node. Then, the authors present a technique to detect the node cloning attack by adding two-hop information to a HELLO message. In particular, the proposed solution requires each node to advertise its two-hop neighbors to enable each node to learn complete topology up to three hops and detect the inconsistency when the node cloning attack is launched. The main advantage of this approach is that it can detect the node cloning attack without using special hardware such as a GPS or requiring time synchronization. One limitation of this approach is that it might not detect node cloning with nodes further away than three hops.

III. Proposed Model

This Proposed Model describes the methodology and contribution of the proposed system. First the overall introduction to the proposed is given, advantage of the proposed system also discussed in this chapter.

3.1.1 Proposed System

The proposed system extends the work on a CCCD (**C**ustomized **C**lock based **C**lone **D**etection) protocol. The protocol performs set of processes which are helped to identify the clone nodes. Applying clock values, port hopping process and resynchronize the node details. The protocol applies the isolation step after detection of clone attacks. So that our protocol's can detect node clone with high security level and holds strong resistance against adversary's attacks.

Base on the clock settings at the server, the nodes send their location and time stamps. This helps to identify the clone nodes in the network.

3.1.2 Advantages

- To performs FCD algorithm to detect mobile clones with minimizing the time.
- The DHT-based protocol can detect node clone with high security level and holds strong resistance against adversary's attacks.
- Randomly directed exploration, is intended to provide highly efficient communication performance with adequate detection probability for dense sensor networks.

3.2 Contributions Of The Proposed work

➢ The system proposing protocol performs set of processes which are helped to identify the clone nodes. Applying clock values, port hopping process and resynchronize the node details.

➢ System enables sensor nodes to distributive construct an overlay network upon a physical sensor network and provides an efficient key-based routing within the overlay network.

➢ Hash table is a decentralized distributed system that provides a key-based lookup service similar to a hash table: (key, record) pairs are stored in the DHT, and any participating node can efficiently store and retrieve records associated with specific keys.

➢ Another port-hopping scheme for the client-server mode proposed this system there; time is divided into discrete time slots. s. The clients and the server share a pseudo-random function to compute which port should be used in a Random Time slot.

➢ System fully decentralized, key-based caching and checking system is constructed to catch cloned nodes effectively. And provide Location Information Exchange Protocol use to exchange some information they are - Time & location in all nodes.

IV. Implementation Of The Proposed work

The CCCD protocol has been applied. Detecting clone attacks is very crucial in WSN due to node mobility. The protocol performs set of processes which are helped to identify the clone nodes.

Clocks of sensor nodes should normally operate unsynchronized at their own pace, but should synchronize whenever Sensors synchronization is needed. Local timestamps of two sensor nodes at the occurrence time of an event are synchronized later by extrapolating backwards to estimate the offset between clocks at a previous time. Our proposed a new technique, called port hopping where the port number used by the server varies as a function of time and a shared secret between the server and the client. Strength of the mechanism lies in the simplification of both the detection and filtering of Clone attacks packets.

Port hopping technique, the port numbers change dynamically as a function of time and key shared between the server and the client. Authorized clients who have the key will be able to determine the current port number used by the server, this scheme, and time is divided into discrete slots time slots for the same service. In order to take into consideration the Time synchronization errors between the server and the client, two ports are used at the boundaries of time slots. Distributed hash table (DHT) by which a fully decentralized, key-based Caching and checking system is constructed to catch cloned nodes. A message associated with a key will be transmitted through the overlay network to reach a destination node that is solely determined by the key; the source node does not need to specify or know which node a message's destination is—the key-based routing takes care of transportation details by the message's key. Distributed hash table is a decentralized distributed system that provides a key-based lookup service similar to a hash table: (key, record) pairs are stored in any participating node can efficiently store and Retrieve records associated with specific keys.

The protocol's performance on memory consumption and a critical security.

The detailed description of the CCPH protocol follows:

Protocol 1: CCPH protocol steps

Input : Node ID of the node. aid: ID of the met node. ta: Present time of node a. CTa : Check.

Table stored in node a memory. RTa: Revoked.

Nodes table stored in node a memory. TTa : Time.

Out table stored in ode a memory. A: Alarm time.G: Time for the clone node to prove its presence.

CCCD steps :

Stage 1: Initialization

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 tediously increasing nonce, a random round seed, and an action time.

Stage 2: Claiming Neighbors 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.

Stage 3: Processing Claiming Messages:

A claiming message will be forwarded to its destination node via intermediate nodes. Only those nodes in the

network layer need to process a message, whereas other nodes along the path simply route the message to temporary targets.

Stage 4: Clock based synchronization:

Based on the clock settings at the server, the nodes send their location and time stamps. This helps to identify the clone nodes in the network. Time synchronization is needed by almost all Clone detection Nevertheless; it is still a challenging task to synchronize the time of nodes in the network, even though loose time synchronization is sufficient for the detection purpose. Hence, as we know that time synchronization algorithms currently need to be performed periodically to synchronize the time of each node in the network.

Distributed Hash Table :

This maps Data items, key value pairs, on node IDs. Key is computed via hash function from string describing data item. Distributed hash table (DHT), by which a fully decentralized, key-based caching and checking system is constructed to catch cloned nodes. The protocol's performance on memory consumption and a critical security metric are 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 simulation results show that the DHT-based protocol can detect node clone with high security level and holds strong resistance against adversary's attacks.

V. Experimental Results

The proposed system efficiency is analyzed using some experimental analysis. The experiments are taken by using the sample input values and the corresponding output values are noted for plot the chart. The following factors

are experimented with some input values to make sure that Quality of Service is achieved in the proposed system.

A. Performance Analysis

For the Customized Clock based Clone Detection protocol, we use the following specific measurements to evaluate its performance:

- Average number of transmitted messages, representing the protocol's communication cost;
- Average Time Delay, 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.

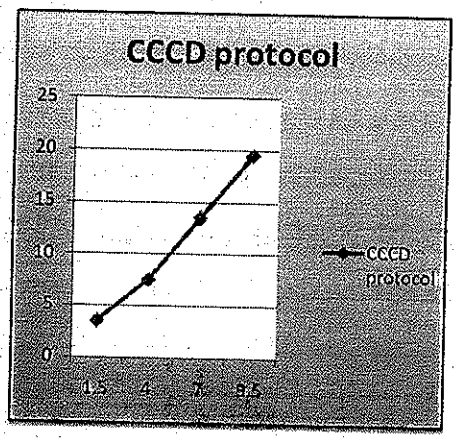

Figure 1: CCCD Protocol

The ratio of number of packets send from source and number of packets reach the destination. The packet delivery ratio is calculated as follows:

PDR = (No of packets Received / No of packets send) * 100

Table 1: PDR Comparison Table

Existing	Proposed
95	99
94	99
92	98
89	97

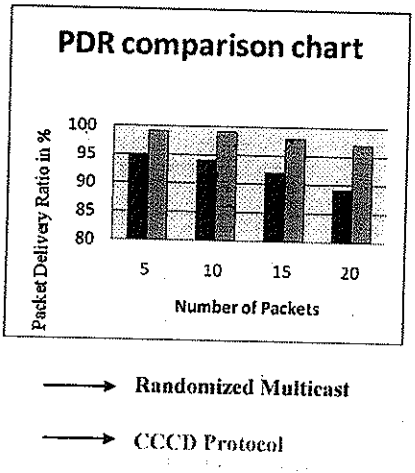

Figure 2: PDR Comparison Chart

In the existing system the packet delivery ratio decreases due to high mobility, security problems and propagation delay in communication even though multiple redundant paths are available. The proposed system Customized Clock based Clone Detection uses to send the packet from source to destination thus the packet delivery ratio increases.

B. Packet overhead :

The number of transmitted routing packets. For example, a HELLO or TC message sent over four hops would be counted as four packets in this metric. Overhead has been plotted against number of nodes.

Delay Time

The proposed system disseminate the message in multiple shortest paths and the message reach the destination in any of the available shortest paths .Thus Delivery time of proposed system increases when compared to the existing system. Delivery time is calculated as follows:

Delivery Time = Receiving time – Sending time

Table 2: Delay Time

Number of receivers	Existing System	Proposed System
5	5	3
10	8	5
15	15	8
20	20	11

The below chart is plotted using the table values which are experimented in the implemented system. The diagram clearly shows that the proposed system have taken less time when compared with the existing system.

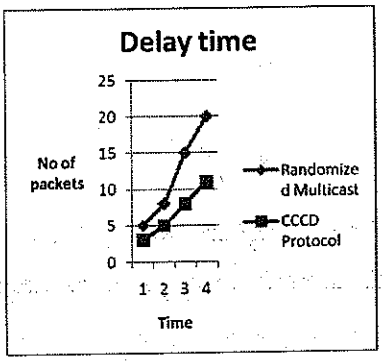

Figure 3: Delay

Table 3: Clone Node Identification Accuracy

Existing system	Proposed system
1.5	3.5
4.0	7.5
7.0	13.5
9.5	19.5

The above table contains the estimated time for detecting the clone nodes in the network by existing and proposed. The plotted chart shows that the proposed system more efficient to detect the clone nodes.

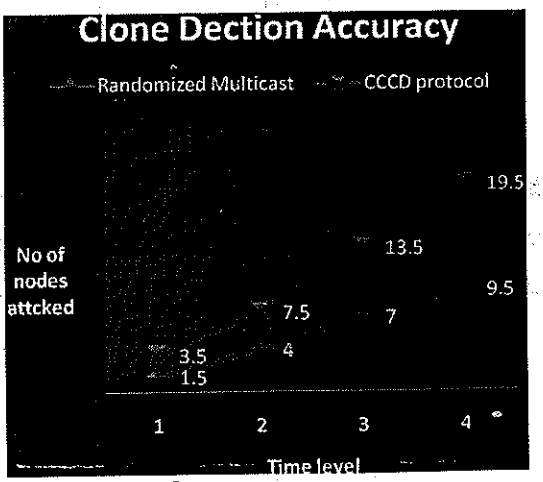

Figure 4: Clone Detection Accuracy

VI. Conclusion

The system has proposed a clone detection scheme for mobile Adhoc networks based on the time synchronization and port hopping schemes with CCCD protocol (Customized Clock based Clone Detection). This also

performs FCD algorithm to detect mobile clones with minimizing the time. So this implemented by using the basic idea that a mobile node should send periodical hopping details according to the clock . The proposed scheme quickly detects mobile clone nodes with very small number of efforts and claims. Furthermore, his also introduces solutions for two types of attacks that might be launched by the attacker and discussed the defense strategies against those node replica attacks. Moreover, the system also indicated that the Simulation and results shows the proposed System finds the attacker with minimum Energy and cost. overhead of the proposed CCPH protocol should not be large. The proposed simulation and results shows the proposed system finds the attacker with minimum energy and cost.

VII. Future Enhancement

The system considered that the ideas and protocols introduced in this paper covered the cost and energy base issues in clone detection system. This provides a way for further research in the area of accuracy; this can be extended by considering the elimination of false alarms. Furthermore, this can be applied and suited to address all major security threats; this can be examined and implemented in real systems.

Furthermore, this can be evaluating the proposed scheme against various types of attacker models. In particular, this can be extended in exploring how a variety of attacker models impact on the security of the scheme.

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 in wireless sensornetworks,"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.

Author's Biography

Jayapriya.M, completed her undergraduate degree from Bharathiar University Arts and Science College, Valparai. And has also completed her post graduate level course M.Sc at Bharathiar University Arts and Science College, Valparai. And is currently pursuing her M.Phil in Computer Science at RVS College of Arts &Science, Coimbatore, India. Her area of interest is Advanced Networking.

Dr B Rosiline Jeetha, graduated B. Sc. (Comp. Sci.) from Madras University, MCA from IGNOU. She obtained her M. Phil., (CS) and Ph. D. (Comp. Sci.) in the area of Data Mining from Bharathiar University, Coimbatore. At present she is working as Associate Professor, Department of MCA in RVS College of Arts and Science, Coimbatore. Her research interest lies in the area of Data Mining.