Article can be accessed online at http://www.publishingindia.com

Clone Detection in Manet Using Routing Information Protocol

Sakthivel Munuswamy*, Anand Joseph Daniel Chinnaiyan, Karnavel Kuppuswamy*****

Abstract

An extensive helplessness of wireless networks in exacting the Mobile Ad-Hoc Network (MANET) is their vulnerability to node compromise and physical capture attacks. Detecting replication attacks is a non-trivial problem in MANETs due to the challenges resulted from node mobility, cloned and compromised node collusion, and the outsized number and extensive of the replicas. It has two replication detection schemes, Time Domain Detection (TDD) and Space Domain Detection (SDD). The theoretical analysis indicates that TDD and SDD provide high detection accuracy and excellent resilience against smart and colluding replicas. They have no restriction on the number and distribution of replicas, and incur low communication and computation overhead.According to theoretical analysis, for validating the path to occur any interference before transmitting the data from source to destinationthe RIP Protocol, TDD and SDD are the only approaches that support mobile networks that places no restrictions on the number and distribution of the cloned frauds and on whether the replicas collude or not.

Keyword: TDD (Time Domain Detection), SDD (Space Domain Detection), RIP (Routing Information Protocol), MANET.

Introduction

MANET is a kind of wireless ad-hoc network, self-forming, self-maintained, and self-healing, allowing for extreme network flexibility. While MANETs can be completely self-contained infrastructure-less network, they can also be tied to an IP-based global or local network. The mobile devices are free to move randomly and arrange themselves randomly. The communication takes place in MANET by using multi-hop paths. Nodes in the MANET share the wireless medium and the topology of the network changes erratically and dynamically. In Mobile Ad-hoc Network (MANET), breaking of communication link often happens, as nodes are free to travel to anywhere. The density of nodes and the number of nodes depends on the applications in which we are using MANET. Many applications there are still some design issues and challenges to overcome (Mohit Kumar andRashmi Mishra, 2012).

We can characterize the life cycle of mobile ad-hoc network into three generations, first, second and third generation. The ad-hoc networks are considered the third generation. The first generation of ad-hoc networks is called Packet Radio Network (PRNET). The Defence Advanced Research Project Agency (DARPA) initiated research of using packet switched radio communication to provide reliable communication between computers and urbanized PRNET. The PRNET is then evolved into the Survivable Adaptive Radio Network (SURAN) in the early 1980's. SURAN provides some benefits by improving the radio performance. Italso provides resilience to electronic attacks. Around the same time, United State Department of Defence (DOD) continued funding for programs such as Globe Mobile Information System (GloMo) and Near Term Digital Radio (NTDR).

* Computer Science, Anand Institute of Higher Technology, Kazhipathur, Tamil Nadu, India. E-mail: sakthikfriends@gmail.com
** Computer Science, Anand Institute of Higher Technology, Kazhipathur, Tamil Nadu, India. E-mail: anandjosephdanield.cse@aiht.ac.in
*** Computer Science, Anand Institute of Higher Technology, Kazhipathur, Tamil Nadu, India. E-mail: treseofkarnavel@gmail.com

NTDR is wear by Army. The functioning group of MANET is born in Internet Engineering Task Force (IETF) who works to standardized routing protocols for MANET and gives rise to the development of various mobile devices like notebooks, PDA's, palmtops etc.

Time Domain Detection

Time Domain Detection (TDD) is the distributed mechanism to detect node replication attacks in MANETs. In this mechanism, time is divided into equal-length intervals and the time intervalsare associated with the challenge. At the beginning of each time interval, trusted node broadcasts the challenge to every node in network. Based on the one-way property of hash chain, it can easily verify the authenticity by using any of the previously verified challenge or the preloaded. Once receiving challenges, node computes a time for each node in the network using the time generation function taking the identity.

Space Domain Detection

Space Domain Detection (SDD) scheme is used for detecting node replication attacks. This detection scheme consists of two phases: the local check phase and the local witness check phase.The local check is the phase when two nodes meet each other and exchange information according to the local information exchange. At the receiver end it checks the authenticity of this message by the public key. If the message fails to pass the authenticity check, receiver end reports an external attack on the source node. Receiver end records its state at the table.

The local witness check is based on the following observation. The witness nodes record the inevitable information during exchanging the information in the node to node. Once the nodes meet each other they exchange the recorded information about identity. They may find the contradictory information by using this replication attacks can be identified.

Routing Information Protocol (RIP)

The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols and employs the hop count as a routing metric. The RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. Maximum number of hops allowed for RIP is 15 and this hop limit also limits the size of the networks that RIP can support. The hop count of 16 is considered an infinite distance, in other words the route is considered unreachable.

RIP implements the route poisoning and hold down mechanisms and split horizon to prevent wrong routing information from being propagated. It is also possible to use the Routing Information Protocol with Metric-Based Topology (RMTI) algorithm to cope with the count-to-infinity problem. It is work able to detect every workable loop with a very small computation effort. The RIP protocol is mainly used for validating the path from source to destination by updating the routing table and calculates the distance between source to destination.

Routing Table

A routing table uses the same idea that one does when using a map in package delivery. Whenever a node needs to send data to another node on a network, it must first know where to send it. If the node cannot directly connect to the destination node, it has to send it via other nodes along a proper route to the destination node. Most nodes do not try to find out which routes might work, instead, a node will send an IP packet to a gateway in the LAN, which then decides how to route the "package" of data to the correct destination. Every gateway will need to keep track of which way to deliver various packages of data, and for this it uses a Routing Table that has a database which keeps track of paths, like an atlas, and allows the gateway to provide this information to the node requesting the information with the hop-by-hop routing. Each routing table maintains lists for all reachable destinations, the address of the next device along the path to that destination: the next hop. Assuming that the routing tables are reliable, the simple algorithm of relaying packets to their destination's next hop thus suffices to deliver data anywhere in a network. Hop-by-hop is the fundamental quality of the IP Internet work Layer and the OSI Network Layer.

Attributes of the Routing Tables are:-

1. Network Number
2. Forwarding MAC Address

3. Hop Count
4. Interface

Objectives of Research

The motivation of this research is to check the behaviour of the system for detecting replicated nodes with the help of TDD and SDD.

- How to detect replicated node?
- Why should the path be validated before sending the data?
- How to manage congestion and collusion during data transmission from source to destination?
- How to provide Guaranty Delivery of data to the MANET users. ?

Literature Survey

- Ryo Murakami, Nariyoshi Yamai and Kiyohiko Okayama. (2010) say that the network consists of collection of interconnected nodes to identify the nodes in the network.
- Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini and Alessandro Mei(2011) say that the replication node can be detected using the RED Algorithm, it is highly efficient in communication memory and computation.
- D.Sheela, Priya darshini and Dr. G.Mahadevan (2011) say that detection of the node is done using Random Witness Selection (RWS) Protocol and Minimized Random Witness Selection (MRWS) protocol. The replicas are then used to launch a variety of attacks that subvert the goal of the sensor application, and the operation of the fundamental protocols. The detection of node duplication attacks in a wireless sensor network is therefore a fundamental problem. The issues of this system lower the communication costs and increase detection rates.
- H. Wen, J. Luo and L Zhou (2011) say that the adversary extracts important security information regarding shared secrets, cryptographic keys and so on and the adversary can easily launch node duplicate attack, which is an attack that anchallenger attempts to add one or more nodes to the network by cloning captured nodes. This type of attack inflicts a severe threat to wireless sensor networks (WSNs). To avoid these issues they introduced the Channel Identification method to detect the clone node in the network. A clone node is distinguished by the channel response which is extracted and used to estimate the channel information between two nodes. Finally, the wireless insite (WI) tools, NS-2, and MATLAB software are employed to test the validity of our scheme under different networks. In addition, our approach incurs much less transmitting data and light overhead. It only overcomes a number of legacy problems in the conventional up-layer clone nodes detection approaches.
- Zeng, Jiannong Cao, Shigeng Zhang, Shanqing Guo and Li Xie(2010) say that the two new NDFD protocols, Random Walk (RAWL) and Table-assisted Random Walk (TRAWL), which fulfill the requirements while having only moderate communication and memory overheads. The additional table is used to maintain all the information about the node. I have additionally occupied the space which requires additional power and space.
- Baisakh, Nilesh Kumar R Patel and Shishir Kumar (2012) say that the energy conscious DSR by not considering power consumption. The two important features of this are energy saving and energy survival. The primary objective of ECDSR is to select the path for the specified source to destination in such a way that all intermediate nodes will have higher level of energy at a given time. So instead of following minimum hop count method during the route discovery phase, select those path whose intermediate nodes are having higher remaining battery power. It analyzes one of the network performance metrics called Packet Delivery Fraction (PDF) which helps to analyze the loss rate of the network. It enhances the lifetime of the network and increases the overall performance.
- Ana Liu, Lin Li, Hongyi Yu and Dalong Zhang(2007) say that the traffic pattern is data gathering from sensor nodes to sink through multi-hop paths forming a tree structure. It incorporates the idea of clustering-based technique in which a parent and its child nodes form a virtual cluster. It aims at reducing the energy for control overhead and collisions. The assumptions are 1. Sensor nodes are stationary; 2. Topology will change only due to nodes exhaust battery energy. Through experimental results it has been proved that better energy efficiency is achieved

in which each node is time-correlated.

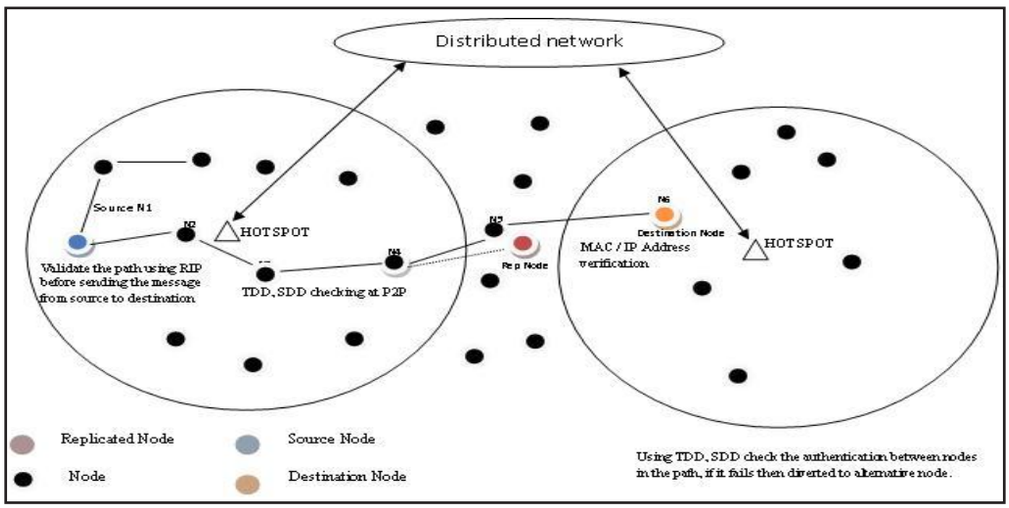
- M. Wang and L. Lamont (2005) say that they provide security mechanism to Optimized Link State Routing Protocol that prevents attacks from intruders with semantic check pointing. Conflict checking based on semantic properties is applied in every MANET node through which any abnormal protocol semantics will trigger an intrusion alarm. The case study shows that the approach effectively enhances security level and fault detection capability of an OLSR protocol. It achieves optimization over LSR through the use of MPRs that are selected and designated by neighboring nodes. MPR nodes declare links in OLSR and only MPR nodes forward messages for those neighbor nodes that selected them as an MPR node.
- Chiung-Ying Wang, Chi-Jen Wu, Guan Nan Chen and Ren-Hung Hwang (2005) say that the significant power consumption and transmission latency, and to achieve efficient power saving. It is a periodically awaken interval protocol, which assumes that beacon intervals of mobile nodes can be synchronized by global synchronization algorithm. A mobile node needs to send beacon packet periodically to remedy drift time with neighbor nodes at each beacon window. Simulation results also show that p-MANET has higher fraction of survived node and lower neighbor discovery time than Quorum-based protocol.
- Kwan-Wu Chin and Darryn Lowe (2005) say that the MANET can continue to operate even when there are conflicting addresses. This paper discusses about the features like enhanced ARP, conflict notification and next-hop forwarding table, shim header, UID role expansion. An enhanced address resolution protocol that prevents contamination of routing tables when neighboring nodes have conflicting addresses. It also maintains IP to MAC address mappings. Conflict avoidance forwarding scheme works together with a routing protocol to build a forwarding table that allows packet delivery even when multiple neighbors share the same IP or MAC address.

Model Construction

Architectural Diagram

Figure 1 represents the architectural diagram. Here user sends the data to the destination in the infrastructure mobile ad-hoc network. The access points are connecting the network to the distributed network. The source nodes validate the path before sending the data.

Figure 1: Architectural Diagram



Once the path has been validated, data are sent to the destination. Each node has the responsiblity to detect the replicated node by using the Time domain detection and Space domain detection. If the replicated node is detected, it checks the replicated nodes information to the nearest node. Based on further processing it is concluded that

the replicated node has been detected. Then it changes the alternate path to reach destination. Another efficient way to detect duplicate nodes at the destination point is to check the MAC and IP address of corresponding destination node. If it is matched then the destination node is the correct node, otherwise it is detected as a replicated node.

Overall Design

Figure 2: Architectural Diagram-II

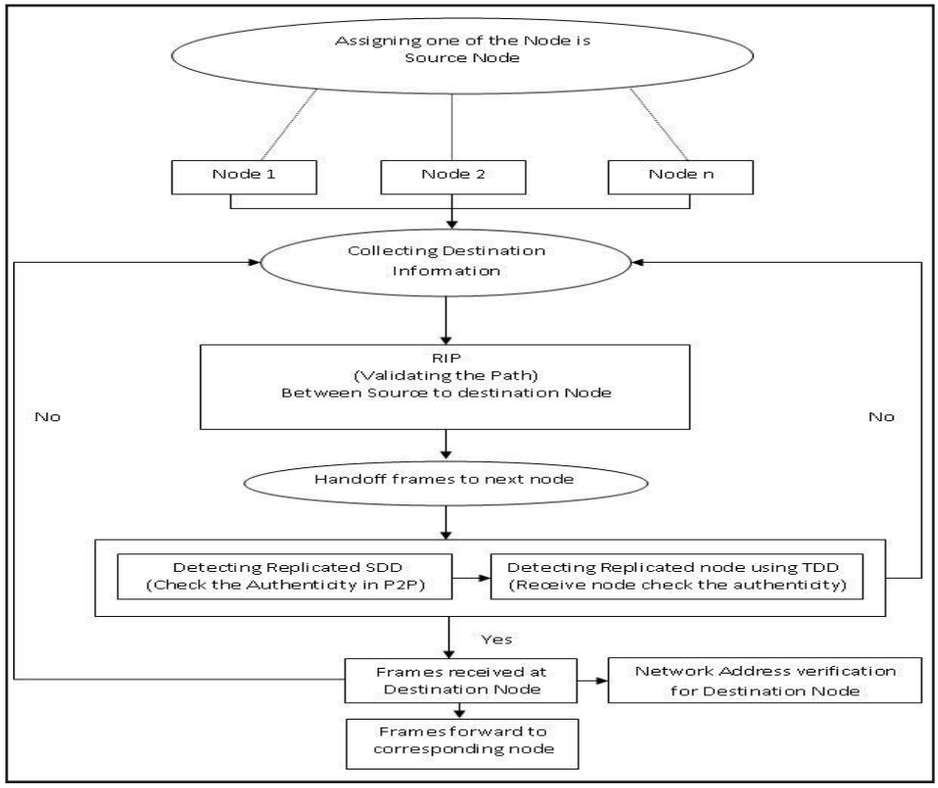


Figure 2 shows the overall description of the clone detection using the routing information protocol. The no. of nodes are interconnected in the Mobile Ad-hoc Network during the data transmission. This model detects the replicated node to provide the guarantee of service.

The source node collects all the information about the destination node to make a connection establishment and to send the data.

It checks the channel and destination node to be idealness by using the Request to Send (RTS) and Clear to Send (CTS). Along with this the RIP Protocol is applied for validating the path and estimate the distance from source to destination before sending the data.

After finding that the destination node is free, RIP protocol is then applied for validating the path and estimate the distance and hop count. Path validation means every routing table share the routing information to the neighbour node with the help of the split horizon, route poisoning and hold down mechanisms to prevent incorrect routing information from being propagated.

After sending the data, collusion and clone node detection are checked with the help of Time Domain Detection. At the beginning of each time interval, the trusted node broadcasts the challenge to every node in network based on the one-way property of hash chain.

It detects the clone node with the help of the local node information and the witness node information that is said to be a Space Domain Detection. At the receiver end it checks the authenticity of this message by the public key. If the message fails to pass the authenticity check, receiver end reports an external attack on the source node. Receiver end records its state at the table.

At the destination side it checks the authentication, IP Address and MAC address verification to confirm that the destination node is a valid node by matching with the MAC address. The clone node has been detected if the MAC address is not matched.

Conclusion

Thus the proposed system detects the replication node in Mobile Ad-Hoc Network (MANET) during data transmission from one node to another. The following methods are used for detecting the replication node: (i) TDD (ii) SDD (iii) Verify MAC and IP Address. Time Domain Detection (TDD) is the distributed mechanism to detect node replication attacks in MANETs. Space Domain Detection (SDD) is used for detecting node replication attacks. This detection scheme consists of two phases: the local check phase and the local witness check phase. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The MAC address is used to find out the actual user or not. One-way property of hash chain can easily verify the authenticity by using any of the previously verified challenge or the preloaded. Once receiving challenges, node computes a time for each node in the network using the time generation function taking the identity. RIP protocol is mainly used before sending the data for validate the path and estimate the distance between source and destination. This will avoid the collusion and other errors over the path. These methods provide support for more secured data transmission from source to destination and also guarantee delivery of packets without loss.

References

Baisakh, P. N. R. & Kumar, S. (2012). *Energy Conscious DSR in MANET*. 2nd IEEE International Conference on Parallel, (December, 784-789).

Choi, H., Zhu, S. & La Porta, T. F. (2007). Detecting Node Clones in Sensor Networks. (Secure Comm 07), (pp. 341-350).

Ganeriwal, S. & Srivastava, M. B. (2004). *Reputation-based Framework for High Integrity Sensor Networks*. University of California.

Ho, J., Wright, M. & Das, S. K. (2009). *Fast Detection of Replica Node Attacks in Sensor Networks Using Sequential Analysis*. Proceedings of IEEE INFOCOM.

Liu, A., Li, L., Yu, H. & Zhang, D. (2007). *An Energy-efficient MAC Protocol Based on Routing Information for Wireless Sensor Networks*. IEEE Communications Society, (March, pp. 458-462).

Murakami, R., Yamai, N. & Okayama, K. (2010). *A MAC-address Relaying NAT Router for PC Identification from Outside of a LAN*. 10th Annual International Symposium on Applications and the Internet, (pp.237-240).

Sheela, D., Priyadarshini. & Mahadevan, G. (2011). *Efficient Approach to Detect Clone Attacks in Wireless Sensor Networks, Electronics Computer Technology* (ICECT). 3rd International Conference, (April, 5, pp.194-198).

Vincenzo, L., Conti, M., Di Pietro, R., Mancini, L. V. & Mei, A. (2011). *Distributed Detection of Clone Attacks in Wireless Sensor Networks*. IEEE Transactions on Dependable & Secure Computing, September/October, 8(5), 685-698.

Wen, H., Luo, J. & Zhou., I. (2011). *Lightweight and Effective Detection Scheme for Node Clone Attack in Wireless Sensor Networks*. IET Wireless Sensors.

Xing, K., Liu, F., Cheng, X. & Du, D. H. C. (2008). *Real-time Detection of Clone Attacks in Wireless Sensor Networks*. 28th International Conference on Distributed Computing Systems (pp. 3-10).

Yang, Y., Wang, X., Zhu†, S. & Cao, G. (2004). *SDAP: A Secure Hop by Hop Data Aggregation Protocol for Sensor Networks*. University of California.

Zeng, Y., Cao, J., Zhang, S., Guo, S. & Xie, L. (2010). *Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks*. IEEE Journals on selected Areas in Communications, June, 28(5), 677-691.

Kumar, M. & Mishra, R. (2012). An overview of MANET: History, challenges & applications. *Indian Journal of Computer Science & Engineering*, February-March, 3(1), 121.

Wang, M., Lamont, L. & Mason, P. (2005). *An Effective Intrusion Detection approach for OLSR MANET Protocol*. IEEE ICNP workshop.

Wang, C.Y., Wu, C. J., Chen, G. N. & Hwang, R. H. (2005). *p-MANET: Efficient Power Saving Protocol for Multi-Hop Mobile Ad Hoc Networks*. 3rd International Conference on Information, Technology & Management.

Chin, K., Lowe, D. & Lau, W. (2005). *Routing in MANETs with Address Conflicts*. The 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (July, pp. 225-236)