AN ENHANCED APPROACH FOR IMPROVE THE PERFORMANCE OF CERTIFICATE REVOCATION SCHEME FOR CREATING ADVERSARY NODES IN MOBILE AD HOC NETWORKS

Dr.R.Reka[1], K.Saraswathi[2]
[1]Associate Professor, Department of Information Technology,
Panimalar Institute of Technology, Chennai.
[2]Assistant Professor, Department of Computer Science,
Nehru Memorial College, Puthanampatti, Trichy

ABSTRACT

Certificate revocation is a major security component in mobile ad hoc networks (MANETs). Owing to their wireless and dynamic nature, MANETs are vulnerable to security attacks from malicious nodes. Certificate revocation mechanisms play an important role in securing a network. When the certificate of a malicious node is revoked, it is denied from all activities and isolated from the network. The main challenge for certificate revocation is to revoke the certificates of malicious nodes promptly and accurately. In this research work, we build upon our proposed scheme, a clustering based certificate revocation scheme, which outperforms other techniques in terms of being able to quickly revoke attackers' certificates and recover falsely accused certificates. However, owing to a limitation in the schemes certificate accusation and recovery mechanism, the number of nodes capable of accusing malicious nodes decreases over time. This can eventually lead to the case where malicious nodes can no longer be revoked in a timely manner. To solve this problem, we propose a new method to enhance the effectiveness and efficiency of the scheme by employing a cluster id and node id to each clusters based approach to restore a node's accusation ability and to ensure sufficient normal nodes to accuse malicious nodes in MANETs. Extensive simulations show that the new method can effectively improve the performance of certificate revocation.

1. INTRODUCTION

MOBILE ad hoc networks (MANETs) have received increasing attention in recent years due to their mobility feature, dynamic topology, and ease of deployment. A mobile ad hoc network is a self-organized wireless network which consists of mobile devices, such as laptops, cellphones, and Personal Digital Assistants (PDAs), which can freely move in the network. In addition to mobility, mobile devices cooperate and forward packets for each other to extend the limited wireless transmission range of each node by multihop relaying, which is used for various applications security is one crucial requirement for these network services Implementing security is therefore of prime importance in such networks. Provisioning protected communications between mobile nodes in a hostile environment, in which a malicious attacker can launch attacks to disrupt network security, is a primary concern. Owing to the absence of infrastructure, mobile nodes in a MANET have to implement all aspects of network functionality themselves. They act as both end users and routers, which relay packets for other nodes. Unlike the conventional network, another feature of MANETs is the open network environment where nodes can join and leave the network freely. Therefore, the wireless and dynamic natures of MANETs expose them

more vulnerable to various types of security attacks than the wired networks.

Among all security issues in MANETs, certificate management is a widely used mechanism which serves as a means of conveying trust in a public key infrastructure, to secure applications and network services. A complete security solution for certificate management should encompass three components: prevention, detection, and revocation. Tremendous amount of research effort has been made in these areas, such as certificate distribution attack detection and certificate revocation Certification is a prerequisite to secure network communications. It is embodied as a data structure in which the public key is bound to an attribute by the digital signature of the issuer, and can be used to verify that a public key belongs to an individual and to prevent tampering and forging in mobile ad hoc networks. Many research efforts have been dedicated to mitigate malicious attacks on the network. Any attack should be identified as soon as possible. Certificate revocation is an important task of enlisting and removing the certificates of nodes that have been detected to launch attacks on the neighborhood. In other words, if a node is compromised or misbehaved, it should be removed from the network and cut off from all its activities immediately. In our research, we focus on the fundamental security problem of certificate revocation to provide secure communications in MANETs.

2. LITERATURE REVIEW

A new network-based Dynamic Channel Assignment (DCA) [1] scheme with the flexible use of Reuse partitioning technique is proposed, namely flexible dynamic reuse partitioning with interference information (FDRP-WI). Many dynamic channel assignment schemes have been proposed and studied to increase the capacity of cellular systems. Reuse partitioning is another technique to achieve higher capacity by reducing the overall reuse distance. In convention, when RP is exploited in DCA, a portion of channels will be assigned permanently to each partitioned region. However, the number of channels assigned to each region may not be optimum due to the uneven and time-varying traffic. In this scheme, channels are open to all incoming calls and no channel allocation for each region is required. As long as the assignment satisfies the co-channel interference constraints, any user from different regions can us e any channel. This scheme aimed to minimize the effect of assigned channels on the availability of channels for use in the interfering cells and to reduce their overall reuse distances. Under both uniform and non uniform traffic distributions, FDRP-WI exhibits outstanding performance in improving the system capacity by reducing the blocking probability.

A fault tolerant distributed dynamic channel allocation scheme [2] which works well under mobile host failures, base station failures as well as communication link failures. This algorithm is based upon the mutual exclusion model where the channels are grouped by the number of cells in a cluster and each group of channels cannot be shared concurrently within the cluster. When many communication sessions happen simultaneously, it is very possible that two neighbouring cells choose a same channel from the limited channel set. This conflict is similar to the mutual exclusion problem. In this algorithm all channels are partitioned into equal sized groups where the number of groups equals the number of the cells in a cluster. The system model is assumed that a cluster is constructed from seven cells. Each channel groups can be occupied by a base station at any time as long as any neighbour is not already holding it. Because each channel group is protected by a critical section, a group can be held by only one base station in a cluster. Through getting permission from all neighbours, the base station can hold the channel group. An efficient fault tolerant distributed dynamic channel allocation scheme for cellular networks based on mutual exclusion paradigm. Since quality of service is also important we can integrate the quality of service and fault tolerant components as the future work of this paper [2].

Quality of Service based dynamic channel allocation protocol [3] for wireless and mobile networks. In recent years, with the study of many channel allocation and handoff strategies for wireless networks to ensure continuous services a guaranteed quality of service to mobile users is essential. Most of the proposed channel allocation schemes do not take the quality of service provisioning into account. G. Arboit et.al [3] proposed a distributed algorithm for dynamic channel allocation with an efficient adaptive channel reservation schema providing continuous quality of service support.

To acquire the low dropping rate, a proper number of channels in the congested cells are reserved for the handoff calls. This number of reserved channels is related to the traffic involved in the network. This proposed algorithm [4] is based upon the mutual exclusion paradigm where all the channels are grouped into three equal groups and any cell in a cluster can hold a channel group as long as no one of its adjacent cells is holding this group. All the base stations in the mobile cellular network are able to acquire a group at the same time considering the mutual exclusion concept. In terms of expected quality of service guarantees, this scheme dynamically adjusts the amount of reserved channels according to the instant traffic situation. Each base station periodically calculates its recent average call dropping rate. Once the average call dropping rate is larger than the target value, the number of reserved channels is decreased. This target value is independently selected by each base station. Base station has the capability of locating a mobile host and predicting a mobile host's movement. If a new connection request from a mobile host which goes ahead to a congested cell (hot cell), it will possibly be blocked by the base station. If mobile host will enter a cold neighbouring cell, the new call request is accepted by the base station. Experimental results indicated clearly that this scheme exhibited a better performance when compared to channel allocation scheme that doesn't support any quality of service. The future for this is as it does not take into account the possibility that the base station or the link failures, designing a quality of service and fault tolerant based dynamic channel allocation scheme can be done.

Wee-Seng Soh et.al [5] used the Genetic Algorithm in order to solve the resource allocation problem. When a channel is blocked and allowed to borrow from the neighbouring cells, a crucial decision in which of the neighbouring cells it has to borrow is done using genetic algorithm. It is an optimization problem. This algorithm [6] uses new genetic operator called Pluck operator which makes the crucial decision of when and which cell to borrow with the future consideration that the borrowing should not lead the network to chaos. It minimizes the number of blocked hosts and improves long-term performance of network. The Pluck operation on genetic algorithm borrows cells or channels with the future consideration derived from past allocation and the cell properties. By adding Pluck operation on Genetic algorithm improved channel borrowing decisions that minimize the number of blocked hosts and maximize performance. The future work suggested for this one is quantification of Pluck operation.

3. ENERGY CONSUMPTION MODEL

All nodes in the cluster are required to participate in each voting, the communications overhead used to exchange voting information is quite high, and it increases the revocation time. Since participation of all nodes in the cluster results in high energy consumption of nodes in the network. However, certificates of both the accused node and accusing node have to be revoked simultaneously. In other words, the accusing node has to sacrifice itself to remove an attacker from the network. Although this approach dramatically reduces both the time required to evict a node and communications overhead of the certificate revocation procedure due to its suicidal strategy, the application of this strategy is limited.

4. NODE JOIN ALGORITHM

The node join algorithm which is carried out by newly joining nodes that enter the network. A newly joining node becomes CH at a constant rate. A node, which has decided not to become a CH itself, will look for other CH nodes in the area. If there are more than two CHs near the node, it will attempt to join two of these clusters by randomly selecting two of their CHs and sending each of them a CM Hello packet. Otherwise, the joining node declares itself as a CH and broadcasts CH Hello packets. When a CM leaves the cluster, it needs to invoke a similar procedure to find out new CHs. If the CM receives no CH Hello packet from its CH for a certain period of time, the CM considers itself having departed from the cluster, and tries to find and join a new cluster. On the other hand, if the CH cannot receive any CM

Hello packets for a while, this implies that no CM is in the cluster, it then inspects the number of neighboring CHs and becomes the CM for those clusters if at least two CHs are found. By implementing the above procedures, the proposed scheme is able to maintain clusters regardless of the node movements, thus enabling it to detect false accusations. Also, since nodes in the WL cannot become CHs, in the case where

CMs lose their CH because the CH has been put into the WL, they can find and join a new cluster by executing the necessary procedures as described above.

CONCLUSION

Finally this research is stating that the system can be maintained as per the requirement when the bandwidth is appropriately utilized and reserved properly for handoff flows. At the same time, the originating flows are also required attention so that the blocking probability is also maintained. The proposed algorithms reserves the bandwidth for the handoff flows based on time, priority and the user mobility and reduces the blocking probability, dropping probability, end-to-end delay and increases the throughput of the system.

REFERENCES

1. H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "A Dynamic Anomaly Detection Scheme for Aodv-Based Mobile Ad Hoc Networks," IEEE Trans. Vehicular Technology,vol. 58, no. 5, pp. 2471-2481, June 2009.

2.H. Yang, J. Shu, X. Meng, and S. Lu, "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 261-273, Feb. 2006.

3. G. Arboit, C. Crepeau, C.R. Davis, and M. Maheswaran, "A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks," Ad Hoc Network, vol. 6, no. 1, pp. 17-31, Jan. 2008.

4. K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks," Proc. IEEE 71st Vehicular Technology Conf. (VTC '10), May 16-19, 2010.

5. Wee-Seng Soh and Hyong S. Kim, "Dynamic Bandwidth Reservation in Cellular Networks using Road Topology based Mobility Prediction".

6. K.Y. Eng, M.J. Karol, M. Veeraraghavan, E. Ayanoglu, C.B. Woodworth, P. Pancha, R.A. Valenzuel, A wireless broadband adhoc ATM local-area network, IEEE Wireless Networks (1995) 161–174.