ISSN: 2349-6495

Cluster Based Id Revocation with Vindication Capability for Wireless Network

S. Janani Devi*

*Assistant Professor, ECE, A.S.L.Pauls College of Engineering and Technology, Tamilnadu, India

ABSTRACT:

The wireless network is more vulnerable in the level of security attacks than the wired networks. Network security is the main challenge in the service of the network. For secure network communications, ID revocation is the mainly used in the network. In this paper, ID revocation issue is proposed to isolate attackers from the network activities. The Cluster-based ID Revocation with Vindication Capability (CIDRVC) scheme. The warned nodes is recovered to take part in the ID revocation process; to enhance the accuracy, we propose the threshold-based mechanism to assess and vindicate warned nodes asattacker nodes or not before relocating them. The performances of our scheme are evaluated by both numerical and simulation analysis. Also proposed the concept of enhancement and compared the PDR, energy consumption between existing and proposed scheme.

Keywords: ID revocation, ad hoc network, PDR, energy consumption.

I. MOBILE AD HOC NETWORK

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, cell phones, 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.

1.1 Network Security

Security is one crucial requirement for these network services. Implementing security is the prime importance in 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.

1.2 Security Solution for Certificate Management:

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.

II. CLUSTER-BASED ID REVOCATION WITH VINDICATION CAPABILITY FOR MOBILE AD HOC NETWORKS

In this project, we compare the advantages and disadvantages between voting-based and non-voting-based mechanisms. The significant advantage of the voting-based mechanism is the high accuracy in confirming the given accused node as a real malicious attacker or not. The decision process is to satisfy the condition of certificate revocation is, however, slow. On the contrary, the non-voting-based method can revoke a suspicious misbehaved node by only one accusation from any single node with valid certification in the network. It is able to drastically simplify the decision making process for rapid certificate revocation as well as reduce the communications overhead. However, the accuracy of determining an accused node as a malicious attacker and the reliability of certificate revocation will be degraded as compared with the voting-based method. In this Project, we propose a Cluster-based ID Revocation with Vindication Capability (CIdRVC) scheme. Like previously proposed cluster-based schemes, clustering is incorporated in our proposed scheme, where the cluster head plays an important role in detecting the falsely accused nodes within its cluster and recovering their certificates to solve the issue of false accusation. On the other hand, CIdRVC inherits the merits of both the voting based and non-voting-based schemes, in achieving prompt revocation and lowering overhead as compared to the voting-based scheme, improving the reliability and accuracy as compared to the non-voting-based scheme. Our scheme can quickly revoke the malicious device's certificate, stop the device access to the network, and enhance network security

2.1 Policies

- Topology Formation
- Detection and trace back of ATTACKS
- Certificate Revocation

1. Topology Formation

Constructing Project design in NS2 should takes place. Each node should send hello packets to its neighbor node which are in its communication range to update their topology.

2. Detection and trace back of ATTACKS

Neighboring nodes detect attacks of attacker node. Each of them sends out an accusation packet to the CA against attacker node. According to the first received packet (e.g., from node B), the CA hold B and M in the WL and BL, respectively, after verifying the validity of node B. The CA disseminates the revocation message to all nodes in the network.

III. CERTIFICATE REVOCATION

To revoke a malicious attacker's certificate, we need to consider three stages: accusing, verifying, and notifying. The revocation procedure begins at detecting the presence of attacks from the attacker node. Then, the neighboring node checks the local list BL to match whether this attacker has been found or not.

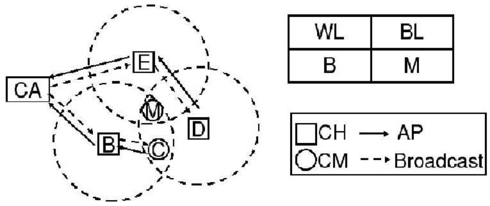


Figure 1: Revoking a node's certificate

To revoke a malicious attacker's certificate, three techniques used: accusing, verifying, and notifying. The revocation procedure begins at detecting the presence of attacks from the attacker node. Then, the neighboring node checks the local list BL to match whether this attacker has been found or not. If not, the neighboring node casts the Accusation Packet (AP) to the CA. The accusing node is held in the WL. Finally, by broadcasting the revocation messages including the WL and BL through the whole network by the CA, nodes that are in the BL are in the BL are successfully revoked from the network.

IV. RESULTS AND DISCUSSION

For evaluating the performance of the Proposed Cluster - based ID Revocation with Vindication Capability for Wireless network is done by using Network Simulator 2. Functionalities of Ns2.33. Network simulator (NS) is an object oriented, discrete event simulator for networking research. NS provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. The simulator is a result of an ongoing effort of research and developed. Even though there is a considerable confidence in NS, it is not a polished product yet and bugs are being discovered and corrected continuously.

NS is written in C++, with an OTcl1 interpreter as a command and configuration interface. The C++ part, which is fast to run but slower to change, is used for detailed protocol implementation. The OTcl part, on the other hand, which runs much slower but can be changed very fast quickly, is used for simulation configuration. One of the advantages of this split-language program approach is that it allows for fast generation of large scenarios. To simply use the simulator, it is sufficient to know. Functionalities for wired, wireless networks, tracing, and visualization are available in NS2.

3.1 Policy 1: ID provided + Hello message

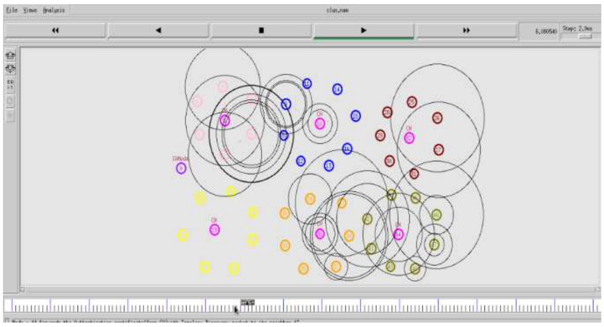


Figure 2 : Hello message + Id provider

This figure 2 shows the scenario of Id provider i.e. Cluster Authority (CA) node is used to generate Id to all other nodes in the network. In this, CA node sends a hello message along with Id in a random number to communicate with other nodes. Nodes cannot communicate with others without valid Id

3.2 Policy 2: Detection of accused nod

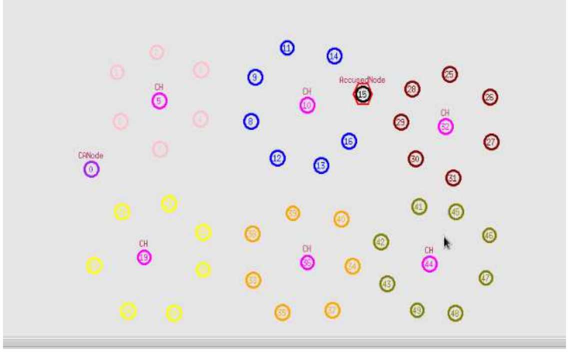


Figure 3: Detection of accused node

This figure 3 shows that the scenario of accused node detection i.e. find the accused node is attacker, CA checks the Id of the accused node with the predetermined value of the node. If the node is attacker then the CH send true message to the authority of the network.

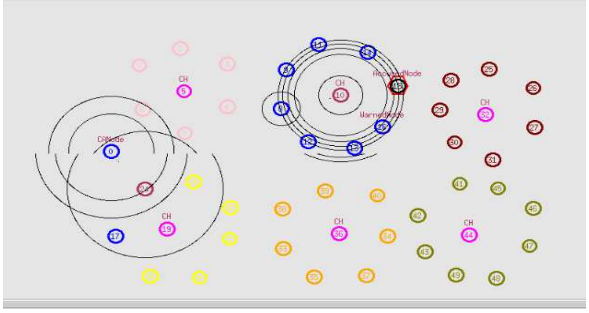


Figure 4: Shortest path to inform about accused node

This fig 4 shows the scenario of shortest path between accused node and the authority node i.e. the information about accused node is send to the authority of the network by shortest path from cluster head and the authority which provide Id to all the nodes. If the accused node is attacker, then true message is send to the authority from header and that attacker node information is passed to all other nodes in the network.

3.3 Policy 3: Revoke the Id of Attacker

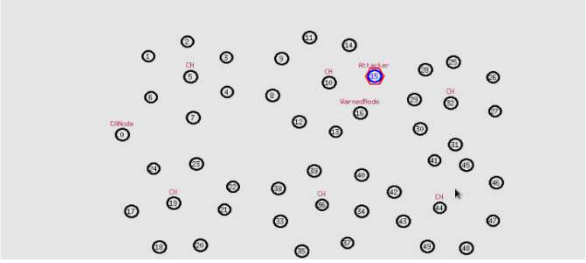


Figure 5 : Revoke the Id of Attacker

This figure shows that the revocation of attackers Id i.e. if the accused node is an attacker then the true message is passed to authority from the CH of the accused node. Then the CA checks the Id with predetermined value and revokes the Id of the attacker and isolates that node from the scenario of the network.

3.4 Energy consumption

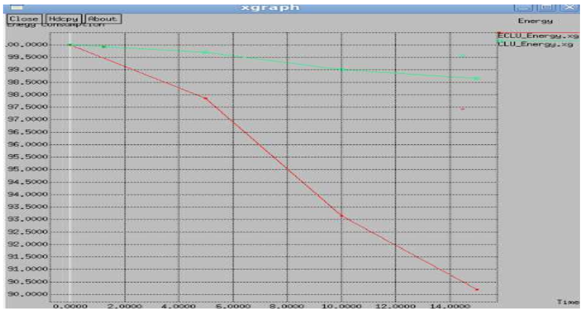
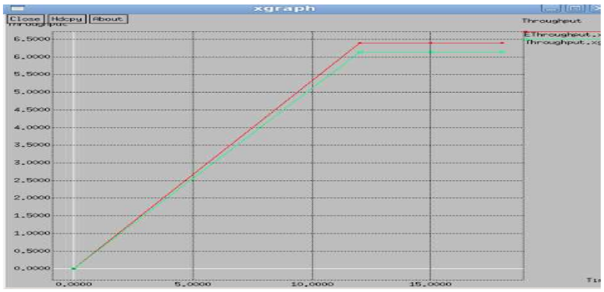


Figure 5: Energy consumption

In this figure 5 , the energy efficiency is compared between existing and proposed scenario. Thus the energy efficiency is high in the CIdRVC scheme when compared to the voting mechanism.

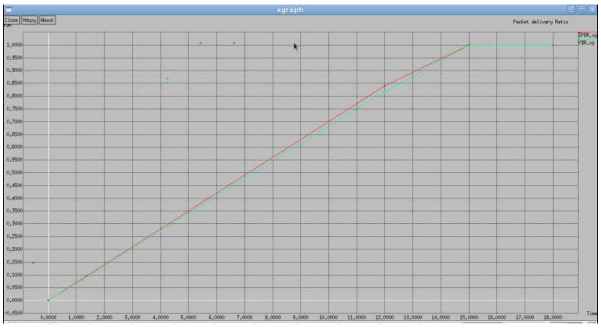
3.5 Throughput of the scenario



Graph 1: Screenshot of Throughput

It is defined as the total number of packets delivered over the total simulation time. The throughput comparison shows that the performance of existing mechanism and proposed method which are very close under of 0 to 49 nodes in MANET scenario Mathematically, it can be defined as: Throughput= N/49 Where *N* is the number of bits received successfully by all destinations.

3.6 Packet Delivery Ratio



Graph 2 : Screenshot of PDR

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. Mathematically, it can be defined as: PDR= *S1*÷ *S2* Where, *S1 is* the sum of data packets received by the each destination and *S2 is* the sum of data packets generated by the each source. Graphs show the fraction of data packets that are successfully delivered during simulations time versus the number of nodes.

V. CONCLUSIONS

The cluster-based Id revocation with vindication capability scheme combined with the merits of both voting-based and non-voting based mechanisms is proposed to revoke malicious certificate and solve the problem of false accusation. The scheme can revoke an accused node based on a single node's accusation, and reduce the revocation time as compared to the voting-based mechanism. In addition, we have adopted the cluster-based model to restore falsely accused nodes by the CH, thus improving the accuracy as compared to the non-voting based mechanism. Particularly, we have proposed a new incentive method to release and restore the legitimate nodes, and to improve the number of available normal nodes in the network. In doing so, we have sufficient nodes to ensure the efficiency of quick revocation. The extensive results have demonstrated that, in comparison with the existing methods, our proposed CIdRVC scheme is more effective and efficient in revoking certificates of malicious attacker nodes, reducing revocation time, and improving the accuracy and reliability of certificate revocation.

REFERENCES

[1]. Luo. H, Lu. S,Yang. H, et al, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Comm., vol. 11, no. 1, pp. 38-47(2012).

[2]. N. Ansari and P. Sakarindr , "Security Services in Group Communications Over Wireless Infrastructure, Mobile Ad Hoc, and Wireless Sensor Networks," IEEE Wireless Comm., vol. 14, no. 5, pp. 8-20, Oct. 2009.

[3]. Hegland A.M, et al, "A Survey of Key Management in Ad Hoc Networks," IEEE Comm. Surveys and Tutorials, vol. 8, no. 3, pp. 48-66, 2011.

[4]. Abdel-Azim M.M , et al,"New Trends in Secure Routing Protocols for Wireless Networks", International Journal of Distributed Sensor Networks, pp. 1-17, 2013.

[5]. Abduvaliyev A, et al, "On the Vital areas of Intrusion Detection Systems in Wireless Sensor Networks", IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, pp. 1223-1237, 2013.

[6]. Alrajeh N.A , et al, "Intrusion Detection Systems in Wireless Sensor Networks: A Review", International Journal of Distributed Sensor Networks, pp. 1-7, 2013.

[7]. Darra E, Katsikas S. K., "Attack Detection Capabilities of Intrusion Detection Systems for Wireless Sensor Networks", IEEE Fourth International Conference on Information, Intelligence, Systems and Applications (IISA), Piraeus, 10-12 July 2013

[8]. Baraani A, H. Jalali, "Process Aware Host-based Intrusion Detection Model", International Journal of Communication Networks and Information Security (IJCNIS) Vol. 4, No. 2, August 2012.

[9]. Chen R.C, et al, "An isolation intrusion detection system for hierarchical wireless sensor networks," Journal of networks, vol. 5, No. 3, pp. 335-342, March 2010.

[10]. Bao F, et al, “Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection,” *IEEE Transactions on Network and Service Management*, vol. 9, no. 2, pp. 169–183, 2012.

[11]. Rottondi C, et al, “Distributed privacy preserving aggregation of metering data in smart grids,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1342–1354, 2013.

[12]. Xi .S and Di X, “A reversible watermarking authentication scheme for wireless sensor networks,” *Information Sciences*, vol. 240, pp. 173–183, 2013.

[13]. Garg R, et al, “An efficient gradient descent approach to secure localization in resource constrained wireless sensor networks,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 717–730, 2012.

[14]. Kim K.J and Hong S.P, “Privacy care architecture in wireless sensor networks,” *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 369502, 7 pages, 2013.

[15]. Cao G and Zhu Z, “Toward privacy preserving and collusion resistance in a location proof updating system,” *IEEE Transactions on Mobile Computing*, vol. 12, no. 1, pp. 51–64, 2013.

[16]. Xiao H, et al, “A new clustering routing algorithm for network based on brief artificial fish-school optimization and ant colony optimization,” *IEEE Transactions on Electronics, Information and Systems*, vol. 133, no. 7, pp. 1339–1349, 2013.