IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Mitigating False Accusations Using Certificate Revocation for High-Throughput Multicast Routing in Wireless Mesh Networks

Divya S Pattathuparambil[*1], Seetha S[2]

[*1,2]Department of Information Technology at Karunya University, India

twinkledsp7@gmail.com

Abstract

Wireless mesh network (WMN) are reliable, multiradio, multihop next generation wireless networks which are capable of delivering high throughput demanded applications through the integration of various technologies. WMN delivers efficient services for a large variety of applications on local, personnel and campus environments. Multicasting is one of the major communication technologies primarily designed for bandwidth conservation and an efficient way of transferring data to a group of receivers in wireless mesh networks. Despite of the vantages of the WMN there can be several issues that affect the entire network performance which include the presence of attackers and the false accusations raised by the nodes. A mere way to identify the malicious node is to collect the information from nodes in the entire network. Nevertheless, in the above said approach, it is difficult to differentiate and identify the valid accusations made by legitimate nodes from false accusations made by malicious nodes. Also, the amount of traffic needed in order to exchange peculiar information on attackers and the necessary time to gather the information increases as the network size becomes more prominent. In this paper, we propose a certificate revocation mechanism which is able to revoke the certification of attackers in a limited period of time with a small amount of controlling traffic. By the clustering of nodes and introduction of multi-level node reliability, the proposed scheme can mitigate the improper certificate revocation due to false accusations by malicious users.

Keywords: Wireless Mesh Networks, Multicast, False Accusation, Clustering, Multiradio.

Introduction

Wireless mesh network [1] is a multiradio multihop network and one of the emerging technologies that are developed to provide solutions to the retreats caused by the wireless adhoc networks. WMN offer high bandwidth, low cost design, all time connectivity features to the wireless network. The main components of WMN include the mesh routers, mesh clients and the gateways where the mesh routers are stationary and form the wireless mesh backbone, which in turn provides the multihop connectivity for the mobile mesh clients to communicate with each other or to the Internet through the access points.

The mesh clients can be mobile or stationary and can form a particular wireless network like adhoc networks, LAN etc. The multihop connectivity of the mesh network provides reliable delivery of information to the proper destination through the intermediate nodes on the course of transmission, even if the specified hosts fails to forward the packets. This explains the major characteristics of wireless mesh networks. WMN are dynamically self-organized, self healing and reliable networks that maintain continuous connectivity among the nodes. These distinguished characteristics of the wireless \ mesh networks make WMN highly reliable and fault tolerant networks.

Figure.1 explains the architecture and communication between the components of WMN.

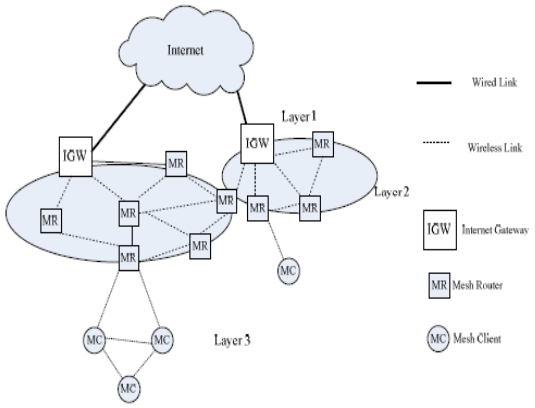

Fig. 1 Wireless mesh network

Multicasting is one of the major applications that are found in mesh networks where the data can be forwarded to a group rather than to a single node

which can increase the entire network performance. Numerous applications in WMN are deployed using multicasting which is feasible in the day to day life, like webcasting, distance learning, online games, and video conferencing. [2].

Related Works

Here, we discuss about several certificate revocation mechanisms. In the mechanism URSA [3], two neighboring nodes receive their certificates from each other and also exchange certificate information about other nodes that they know. Nodes that share the same certificate information are assumed as belonging to the same network. In those networks, the certificate of a suspected node in the network can be revoked when the number of accusations against the node exceeds a certain threshold which can be a predefined value. Even though URSA does not require any special equipment such as Certificate Authorities (CA), the operational cost is still high.

In contrast, DICTATE [4] employs a number of CAs to efficiently perform the publication and revocation of certificates in the network. CAs continuously monitor node behavior to detect attacks and spontaneously share the certificate information between each other. If a CA identifies a malicious node, the certificate of the node is revoked by the CA and its information is shared among other CAs, and thus results in the deletion of the node from the network. However, the deployment of a sufficient number of CAs is not an easy and simple task in WMNs.

In another technique [5], the certificate of a node which has been accused by just one node will be revoked by every node. As a result, this particular scheme exhibits good performance in terms of promptness and low operating overhead compared to other previous prevailing techniques. However, this peculiar scheme has a controversial point where an accuser will be removed from the network along with the accused node. Since this approach is fundamentally flawed, this scheme cannot be commonly used.

The method proposed in [6] introduces a time session above all other techniques to refresh the certificate information of each node. The accusation count is reset at the end of each session by each node. Therefore, while this scheme is able to mitigate the damages caused by false accusations, the performance can be largely degraded by the increase of malicious nodes.

In the voting based scheme [7], [8], if the number of nodes, which have accused a particular node, exceeds the predefined threshold, the accused node is removed from the network by having its certificate revoked. This scheme takes into account of the false accusations, i.e., each accusation has a different weight according to the accuser's reliability. This scheme has two problems, a large amount of operational traffic and a long revocation time, because the opinion of every node in the network is needed for each node to decide whether to revoke the certificate of the malicious node or not. According to the above discussion, in this paper, we propose a certificate revocation scheme which can achieve prompt revocation, lower operational traffic, and mitigate damage from false accusations.

Proposed System

Several prevailing multicast protocols dissent in their metrics consideration and their yield in the throughput. Based on the comparison among various multicast protocols ODMRP [9] provides high throughput when the current metric used is upgraded to the multicast level. The metric that was considered by ODMRP, ETX which is the unicast metric that considers the forward and the backward data flow including the acknowledgement from the receiver nodes.

$$\text{ETX} = \frac{1}{df \text{x} dr} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

Upgrading the ETX metric to a new level SPP, a multicast metric which considers only the forward direction of data transfer helps to replace the former metrics to a new level in the area of WMN.

SPP= *df*.…… (2)

In this modified high throughput ODMRP protocol, as required by the link-quality metric, each node present in the network measures the quality of the links from its neighbors to itself, based on the periodic probes and the messages sent by its most adjacent neighbors. The JOIN QUERY message is flooded periodically by the source S and contains a route cost field which accumulates the metric for the route on which the message traveled. Upon receiving a JOIN QUERY, a node updates the route cost field by accumulating the metric of the last link traveled by the message.

Because different paths may have different metrics, JOIN QUERY messages are flooded using a weighted flood suppression mechanism, in which a node processes flood duplicates for a fixed interval of time and rebroadcasts flood messages that advertise a better metric (indicated by the route cost field). Each node also records the node from which it received the JOIN QUERY with the best quality metric as its upstream node for the source S. After waiting for a fixed interval of time, during which it may receive

several JOIN QUERY packets that contain different route metrics, a multicast receiver records as its upstream for source S the neighbor that advertised the JOIN QUERY with the best metric.

Just like in ODMRP, the receiver then constructs a JOIN REPLY packet, which will be forwarded toward the source on the optimal path as defined by the metric and will activate the nodes on this path as part of the FORWARDING GROUP. In Fig. 2, we give an example of how ODMRP-HT selects the mesh of nodes in the FORWARDING GROUP based on the SPP link-quality metric.

WMN are a highly pliable network where nodes can freely move and join among themselves, without any fixed infrastructure, and thus the vulnerability to attacks by malicious users increases. Therefore, ensuring network security is one of the major issues in WMN. Although a large number of methods to detect various kinds of attacks have been proposed and developed for WMNs, only detecting and blocking those attacks in each node is not enough to maintain network security for attackers can freely move and repeatedly launch attacks against different nodes.

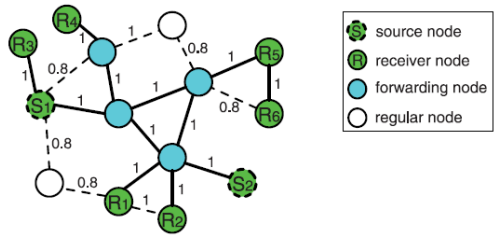

Fig.2 ODMRP- HT Mesh creation with two sources and six receivers

S-ODMRP ensures the delivery of data from the source to the multicast receivers even in the presence of Byzantine attackers, as long as the receivers are reachable through nonadversarial paths. To achieve this, S-ODMRP uses a combination of authentication and rate limiting techniques against resource consumption attacks and a novel technique, RateGuard, against the more challenging packet dropping and mesh structure attacks, including metric manipulations and JOIN REPLY dropping. S-ODMRP uses source message authentication to avoid processing unauthenticated messages.

This eliminates a large class of attacks, including outsider attacks, message spoofing and modification attacks targeting JOIN QUERY and JOIN REPLY messages, and the injection of corrupted data packets. Even with message authentication, an insider attacker can still mount the resource consumption attack by flooding JOIN QUERY messages frequently with itself as the source. Such an attack can be countered by rate limiting; for example, an honest node only forwards JOIN QUERY messages for a source node up to a maximum frequency. To address the resource consumption attack in which the attacker activates many unnecessary data delivery paths by injecting many JOIN REPLY messages, we can limit to at most one the number of JOIN REPLY messages a node may send in one round.

Each node monitors the number of different signed JOIN REPLY messages that originate from its neighbors. If a node is observed to have broadcast two or more different signed JOIN REPLY messages, then punitive actions can be taken against the node (e.g., isolation). The attacks on the mesh structure and packet dropping attacks are much more challenging to defend against, particularly, in the context of high-throughput metrics. In the following, we focus on defending against these attacks. We will first present the high-level overview of our defense scheme, RateGuard, and then present the details of S-ODMRP with the RateGuard scheme.

The rate guard mechanism consists of mainly two phases including the measurement based attack detection mechanism and the accusation based attack reaction mechanism. In the former phase the presence of the attacker is identified on the basis of PDR value that is estimated. The nodes can estimate the expected PDR (ePDR) value and the perceived PDR value (pPDR) which is compared with a threshold value, from which the attack presence is identified. The accusation mechanism is included to recover the network from the attacker nodes up on identifying them where the normal nodes can identify and accuse the attacker nodes.

In implementing such a mechanism there is the risk of accusing normal nodes by the attacker nodes which can produce enormous amount of false accusation packets, which will result in the degradation of network performance and includes several loopholes where the attackers can induce malicious behavior in the network.

Envisioned System

To reduce the damage from attacks, attackers must be immediately found and removed from the network after detection of the first possible attack; this can be achieved by using a certification system in the particular network. In networks employing a certification system, nodes cannot communicate with each other without a valid certification. In other words, any attacker cannot exist in the network once its malicious behavior has been detected by other nodes and its certification has been revoked accordingly by the system.

The method [10] provides the idea of clustering the entire nodes present in the network based on the transmission range of each node. Based on the reliability value of each node the nodes can be classified as normal nodes, warned nodes and the attacker nodes. The energy of the nodes most probably the power can be considered as the energy value which can be measured in Joules. The nodes can be divided as the in to cluster heads (CH) and the cluster members (CM) based on their reliability value. The cluster heads are the normal nodes that have high reliability.

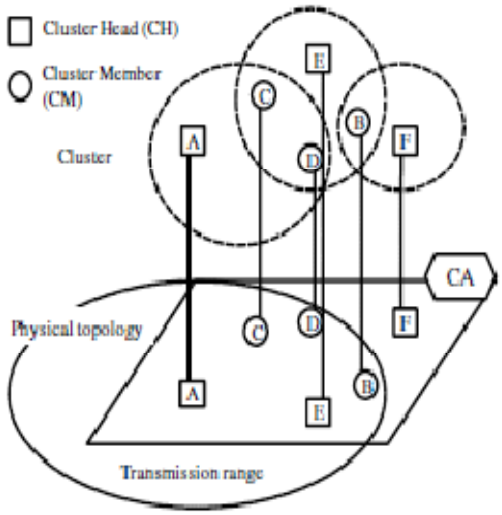

Fig.3 Node Clustering

The cluster head can continuously monitor their members, false accusations produced etc. the certificate authority (CA) can inform the cluster head about any misbehavior. In case of the malicious behaviors and the accusations the nodes are classified as warned nodes and the attacker nodes and are placed in special lists called warned list (WL) and the attacker list or the accused list (AL). Warned list can contain the normal nodes that are accused by the attacker nodes. It is the function of the Certificate authority to notify the cluster head on the accusation of the false accusation and the cluster head can identify the false accusations since it continuously monitors its cluster members. The recovery is done by the Cluster Head using the certificate recovery packets. The Cluster Heads and the Cluster Members communicate through the CH Hello Packet and CM Hello Packet.

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.

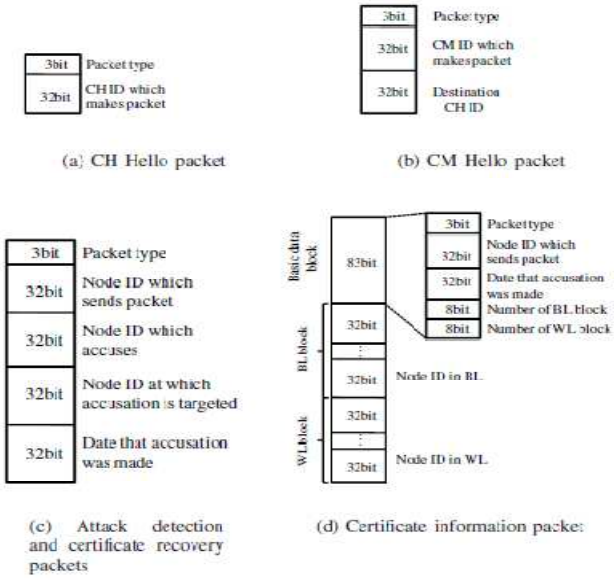

Fig.4 Control Packets

Security Analysis

Through this envisioned scheme gives high throughput and improved security level for the WMN by mitigating the problem of occurring of false accusations in the network through certificate revocation mechanism for each accused nodes.

Performance Simulation

A. Simulation Setup

The simulation was done using the Qualnet in an area of about 100x100 nodes. The attacker nodes are identified based on the PDR value obtained from the metric values based on the ePDR and the pPDR value. The routers and the end devices are configured with limited mobility and power constraints.

B. Simulation Specification

Simulation Field	100mx100m
Transmission range	250m
Energy Level	5.05J/s
Number of Nodes	100
Node Placement	Random

Mobility Model Random-Waypoint

Routing Protocol S-ODMRP

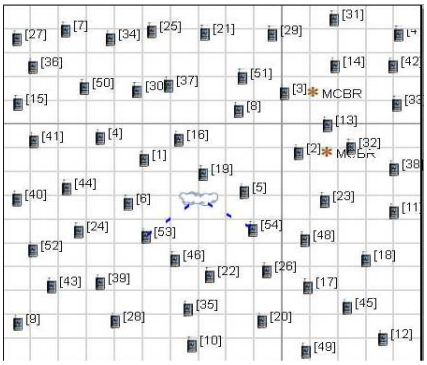

Fig.5 Simulation Setup

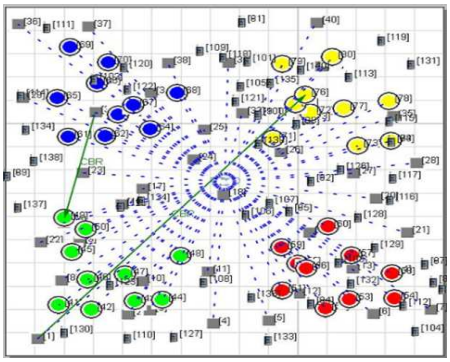

Fig.6 Clustering

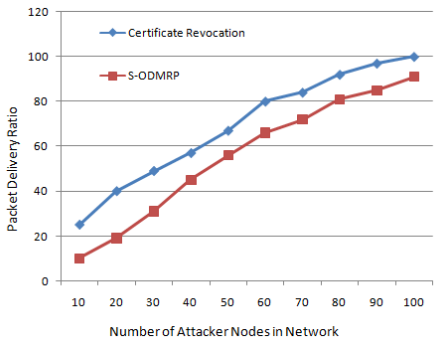

Fig.7 Throughput Graph

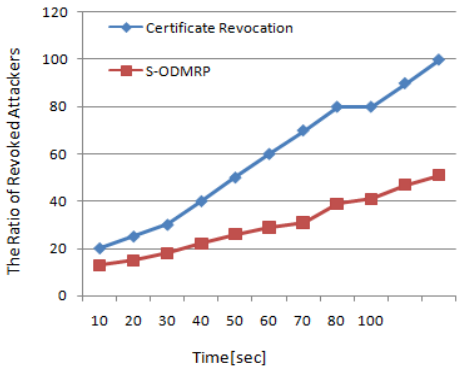

Fig.8 Ratio of Revoked Attackers over Time

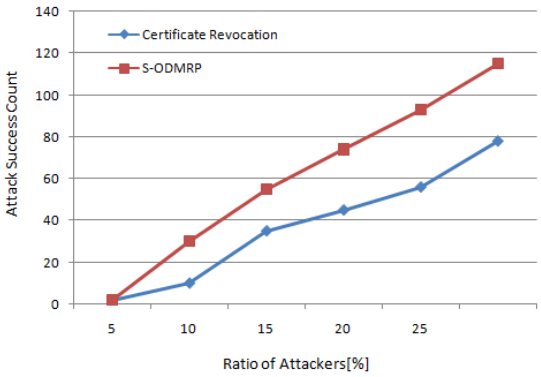

Fig.9 Attack Success count by ratio of Attackers

Conclusion

The method proposes a integrated idea of secure protocol and the clustering mechanism where the malicious behavior of the nodes are removed to a great extent. The paper gives the prominent idea that can be implemented to implement a high throughput and secure network.

References

[1] Benyamina, D, Hafid, A., Gendreau,M., " Wireless Mesh Networks- A Survey" , in journals and magazines IEEE, Volume14, 2012

[2] Akyildiz,I.F. , Xudong Wang, "A Survey on Wireless Mesh Networks" in Journals and Magazines IEEE, Volume 43, 2005

[3] H. Luo, J. Kong, P. Zerfos, S. Lu and L. Zhang, "URSA: ubiquitous and robust access control for mobile ad hoc networks," IEEE/ACM Trans. Networking, vol. 12, no. 6, pp.1049-1063, Oct. 2004.

[4] J. Luo, J. P. Hubaux and P. T. Eugster, "DICTATE: DIstributed CerTification Authority with probabilisTic frEshness for ad hoc networks," IEEE Trans. Dependable and Secure Computing, vol. 2, no. 4, pp.311- 323, Oct.-Dec. 2005.

[5] J. Clulow and T. Moore, “Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems,” ACM SIGOPS Operating Systems Reviews, vol. 40, no. 3, pp.18-21, Jul. 2006.
[6] H. Chan, V. D. Gligor, A. Perrig and G. Muralidharan, “On the distribution and revocation of cryptographic keys in sensor networks,” IEEE Trans. Dependable and Secure Computing, vol. 2, no. 3, pp.233-247. Oct.-Dec. 2005.
[7] C. Crepeau and C.R. Davis, “A Certificate Revocation Scheme for Wireless Ad Hoc Networks,” Proc. of ACM Workshop Security of Ad Hoc and Sensor Networks, 2003.
[8] 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.
[9] Jing Dong, Reza Curtmola, “Secure High-Throughput Multicast Routing in Wireless Mesh Networks” IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 5, MAY 2011.
[10] Kyul Park, Hiroki Nishiyama, Nirwan Ansari, Nei Kato, “Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks”, IEEE Proceedings 2010