International Journal of Science and Engineering Research (IJ0SER),

Vol 3 Issue 9 September-2015
3221 5687, (P) 3221 568X

Certificate Revocation for Mobile Ad Hoc Networks

B.Christopher Paul Kumar
Department of Computer science,
Anna university, Chennai.
India.

Abstract— **Mobile ad hoc networks (MANETs) have attracted much attention due to their mobility and ease of deployment. However, the wireless and dynamic natures render them more vulnerable to various types of security attacks than the wired networks. The major challenge is to guarantee secure network services. To meet this challenge, certificate revocation is an important integral component to secure network communications. In this paper, we focus on the issue of certificate revocation to isolate attackers from further participating in network activities. For quick and accurate certificate revocation, we propose the Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme. In particular, to improve the reliability of the scheme, we recover the warned nodes to take part in the certificate revocation process; to enhance the accuracy, we propose the threshold-based mechanism to assess and vindicate warned nodes as legitimate nodes or not, before recovering them. The performances of our scheme are evaluated by both numerical and simulation analysis. Extensive results demonstrate that the proposed certificate revocation scheme is effective and efficient to guarantee secure communications in mobile ad hoc networks.**

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, 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 multi hop relaying, which is used for various applications e.g., disaster relief, military operation, and emergency communications. Security is one crucial requirement for these network services. Implementing security [1], [2] 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 [3], [4] 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 [5], [6], attack detection [7], [8], [9], [10], and certificate revocation [11],[12], [13], [14], [15], [16], [17]. 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 who 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

RELATED WORK

Recently, researchers pay much attention to MANET security issues. It is difficult to secure mobile ad hoc networks, notably because of the vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, and the lack of infrastructure. Various kinds of certificate revocation techniques have been proposed to enhance network security in the literature. In this section, we briefly introduce the existing approaches for certificate revocation, which are classified into two categories: voting based mechanism and non-voting-based mechanism.

VOTING-BASED MECHANISM

The so-called voting-based mechanism is defined as the means of revoking a malicious attacker's certificate through votes from valid neighboring nodes. URSA [14] proposed by Luo et al. uses a voting-based mechanism to evict nodes. The certificates of newly joining nodes are issued by their neighbors. The certificate of an attacker is revoked on the basis of votes from its neighbors. In URSA, each node performs one-hop monitoring, and exchanges monitoring information with its neighboring nodes. When the number of negative votes exceeds a predetermined number, the certificate of the accused node will be revoked. Since nodes cannot communicate with others without valid certificates, revoking the certificate of a voted node implies isolation of that node from network activities. Determining the threshold, however, remains a challenge. If it is much larger than the network degree, nodes that launch attacks cannot be revoked, and can

successively keep communicating with other nodes. Another critical issue is that URSA does not address false accusations from malicious nodes.

The scheme proposed by Arboit et al. [15] allows all nodes in the network to vote together. As with URSA, no Certification Authority (CA) exists in the network, and instead each node monitors the behavior of its neighbors. The primary difference from URSA is that nodes vote with variable weights. The weight of a node is calculated in terms of the reliability and trustworthiness of the node that is derived from its past behaviors, like the number of accusations against other nodes and that against itself from others. The stronger its reliability, the greater the weight will be acquired. The certificate of an accused node is revoked when the weighted sum from voters against the node exceeds a predefined threshold. By doing so, the accuracy of certificate revocation can be improved. However, since all nodes are required to participate in each voting, the communications overhead used to exchange voting information is quite high, and it increases the revocation time as well.

NON-VOTING-BASED MECHANISM

In the non-voting-based mechanism, a given node deemed as a malicious attacker will be decided by any node with a valid certificate. Clulow et al. [16] proposed a fully distributed "suicide for the common good" strategy, where certificate revocation can be quickly completed by only one accusation. 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. Furthermore, this suicidal approach does not take into account of differentiating falsely accused nodes from genuine malicious attackers. As a consequence, the accuracy is degraded.

Manet Mobile Ad Hoc Network Overview

Mobile Ad Hoc Network (MANET) is a collection of mobile hosts that form a temporary network without centralized administration. In a MANET, nodes within their wireless transmitter can communicate with each other directly while nodes outside the range have to rely on some other nodes to relay messages. When a multi hop scenario occurs, the packets sent by the source multitude are relayed by several intermediate hosts before reaching the destination host. The success of communication depends on the other nodes cooperation.

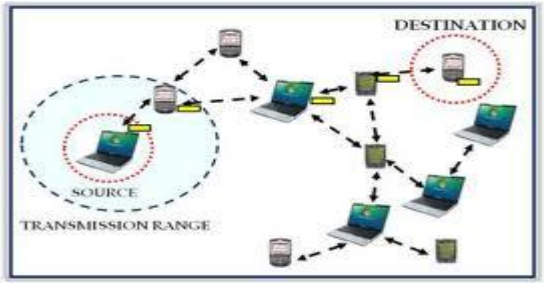

Figure 1.1Mobile ad hoc network

In figure 1.1 shows the MANET, it may be characterized as dynamic, because it continuously changes the mobility of nodes. Also MANET has resource restraint, which imperfect bandwidth and limited battery power. Routing protocols rely on cooperation between nodes due to lack of a centralized administration and assume that all nodes are trustworthy and obedient. Hence replication occurs that means replica of data that will be stored both in the base station and also in the application server which occupies wide memory spaces.

In MANET, each node not only acts as the end system, but also acts as a router, that forwards packets to desired destination nodes. These nodes are capable of both single and multi-hop communication. Mobility and the nonattendance of any fixed communications make MANETs extremely prominent for military and keep operations, sensor networks and time-critical applications. In military, the mobile ad hoc network wear to form the network with the coordination of all members in the team while the time of attack the enemy.

Generally, the hidden and exposed problems are raised in the mobile ad hoc network. In the hidden terminal problem while other sender in sequence is hidden from the present sender, so that transmissions at the same receiver cause collisions. Consider the case of 3 terminals are communicated such as A, B and C The transmission range of A reaches B, but not c. The transmission range of C reaches B, but not C. i.e., A cannot identify C and vice versa.

The terminal A sends to B and C which does not receive this transmission. Terminal C also wants to send something to B and senses the standard. The intermediate appears to be free, the carrier sense fails. C also starts sending causing at B and continues with its transmission. A is concealed for C and vice versa.

While hidden terminal may basis collisions, the next consequence only causes unnecessary delay. If the node B sends data to A, and C wants to transmit data to some other mobile phone outside the intervention ranges of A and B. C sends the carrier and detects whether the carrier is active. C postpones its transmission until it detects the medium as being idle again. But as A is external the intervention range of C, for the prospect is not crucial. Causing a collision is too weak to disseminate to A. C is exposed to B called Exposed Terminal Problem i.e., the sender incorrectly thinks the medium is in use, so that it without cause refers the transmission.

Features of MANET

- Roads less network of mobile devices associated by wireless link.
- No federal administration.
- Limited resources.
- Uncontrolled moving pattern
- Routable networking atmosphere

Applications of MANET

- Cell phone, Laptop.
- Military battlefield network.
- Meetings/conferences.
- Policing and fire fighting.

Objective of the Project

Mobile Ad hoc Network (MANET) can be improved by avoiding the packet forwarding via high power nodes. It can be implemented by developing the new routing protocol for loose virtual clustering routing protocol for power heterogeneous and gain the energy- efficiency in the mobile ad hoc network.

Power Heterogeneous MANETs

In MANET, the mobile network consists of devices with heterogeneous characteristics in terms of transmission power, energy, capacity, radio, etc. The Vehicular Ad Hoc Networks (VANETs), also composed of heterogeneous wireless tools carried by humans and vehicles are derived from power heterogeneous MANETs.

In MANET, the unidirectional links provides the poor performance and it need to detect the unidirectional links and to stay away from the transmissions based on asymmetric links without the high power nodes. Here, the problem is to enhance the routing performance of heterogeneous MANETs. Generally, some routing protocols are used for power heterogeneous MANETs.

Bluetooth

- common short-range wireless capability
- Uses 2.4-GHz band
- accessible globally for unlicensed users
- Devices within 10 m can split up to 720 kbps of power
- Supports unlimited list of applications
- Data, audio, graphics, video

Bluetooth is the best example for mobile ad hoc network, piconet is the coexistence of multiple accesses by provided that the dissimilar hopping patterns to each devices. Bluetooth is the straightforward and inexpensive device for data transferring within the 100m distances.

Bluetooth channels employ a Frequency-Hop/Time-Division-Duple(FH TDD) method in which the time is separated into 625sec intervals called slots. The master to slave transmission starts in even number slots, while the slave to master transmission starts in odd numbered slots. Masters and slaves are allowable to send 1, 3, or 5 slot packets, which are transmitted in consecutive slots. Packets can bring synchronous information (voice link) or asynchronous information. Information can only be exchanged between a master and a slave.

A slave is permissible to start transmission in a given slot if the master has addressed it in the preceding slot. The master addresses a slave by sending a data packet or, if it has no data to send, a 1 slot POLL packet.

The slave ought to respond by shift a data packet, if it has nothing to send, a slot NULL packet. The master to slave announcement as downlink and to the slave to master communication as and it focus on networks in which only data links are used. Different packet generation scenarios: Symmetrical piconet-the arrival rate to every downlink and uplink queue. Half-symmetrical piconet-The arrival rate to all the downlink queues is the same.

1.2.1 Bluetooth Working principle

The Bluetooth protocol operates at license free bandwidth 2.4GHz in the same unlicensed ISM frequency band where RF protocols like ZigBee and WiFi. There is a standardized set of rules and specifications that differentiates it from other protocols.

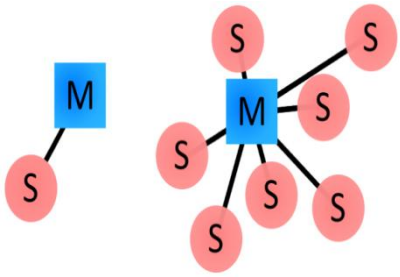

Figure 1.3 Examples of Bluetooth

In figure 1.3, Bluetooth networks (commonly referred to as piconets) use a master/slave model to control when and where devices can send data. In this model, a lone master device can be associated to up to seven different slave devices. Several slave devices in the piconet can only be connected to a single master.

The master coordinates communication throughout the piconet. It can send data to any of its slaves and request data. Slaves are only allowed to transmit to and receive from their master.

Bluetooth Addresses and Names

Every particular Bluetooth device has a unique 48 bit address. This will usually be presented in the form of a 12-digit hexadecimal value. The most-significant half (24 bits) of the address is an organization unique identifier (OUI), which identifies the producer. The lower 24-bits are the more unique part of the address. The "000666" portion of that address is the OUI of Roving Networks, the producer of the module.

Every RN module will contribute to those upper 24-bits. The "422152" portion of the module is the more unique ID of the device. Bluetooth devices can also have user-friendly names known to them. These are usually accessible to the user, in place of the address, to help identify which device it is. The rules for device names are less strict. They can be up to 248 bytes extended, and two devices can share the same name. The unique digits of the address might be included in the name to help distinguish devices.

Connection Process

Bluetooth connection progressive states:

Inquiry – If two Bluetooth devices know absolutely nothing concerning each other, one must run an inquiry to try to determine the other. One device sends out the investigation request, and a few devices listening for such a request will respond with its address, and perhaps its name and other information.

Paging (Connecting) – Paging is the enlargement of forming a connection between two Bluetooth approach. Before this connection can be initiated, each device needs to know the address of the other (found in the inquiry process).

Connection – After a device has concluded the paging process, it enters the connection state. While connected, devices can either dynamically participating or it can be put into a low power sleep mode.

Active Mode – This is the regular connected mode, where the device is actively transmitting or receiving data.

Sniff Mode – This is a power-saving mode, where the device is fewer active. It'll sleep and only pay attention for transmissions at a set interval (e.g. every 100ms).

Hold Mode – Hold mode is a impermanent, power-saving mode where a device sleeps for a defined period and then income back to active mode when that interval has approved. The master can command a slave device to hold.

Park Mode – Park is the deepest of sleep modes. A master can control a slave to "park", and that slave will become inactive in anticipation of the master tells it to wake back up.

Bonding and Pairing

When two Bluetooth devices share a special affinity for each other, they can be bonded together. Bonded devices automatically establish a connection whenever they are closing adequate. When I start up my car, for example, the phone in my pocket immediately connects to the car's Bluetooth system. No UI interactions are required.

Bonds are created through one-time a process called pairing. When devices pair up, they share their addresses, names, and profiles, and usually store them in memory. They also share a common secret key, which allows them to bond whenever they're together in the future.

Pairing usually requires an authentication process where a user must validate the association between devices. The flow of the authentication process varies and usually depends on the boundary capabilities of one device or the other. Pairing is a straightforward "Just Works" operation, where the click of a button is all it takes to pair. Other times pairing involves matching 6-digit numeric codes. Older, inheritance (v2.0 and earlier), pairing processes involve the entering of a common PIN code on each device. The PIN code can range in length and complexity from four numbers (e.g. "0000" or "1234") to a 16-character alphanumeric string.

Time division multiple access (TDMA)

The time division multiple access (TDMA) channel access scheme is based on the time-division multiplexing scheme, which provides dissimilar time-slots to dissimilar data-streams (in the TDMA case to different transmitters) in a cyclically recurring frame structure.

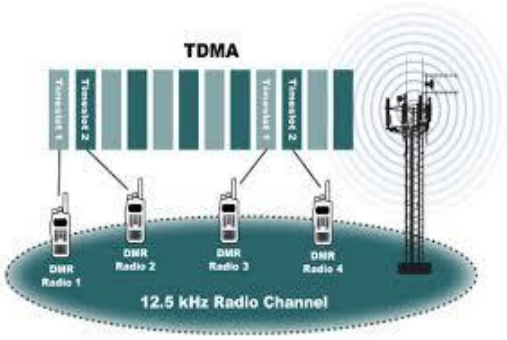

Figure Time division multiple accesses

For example, node 1 may use time slot 1, node 2 time slot 2, etc. in anticipation of the last transmitter. Then it starts all above again, in a repetitive pattern, until a connection is ended and that slot becomes free or assigned to another node. An advanced form is Dynamic TDMA, where a scheduling may give different time but sometimes node 1 may use time slot 1 in first frame and use another time slot in next frame.

In TDD interactions, all directions of transmission use one contiguous frequency allocation, but two separate time slots to provide both a forward and invalidate link.

Since transmission from mobile to BS and from BS to mobile alternates in time, this scheme is also known as "ping pong".

As a consequence of the use of the same frequency band, the statement quality in both directions is the same. This is different from FDD.

shows the 2G cellular systems are based on a combination of TDMA and FDMA. Each frequency channel is separated into eight time slots or seven are used for seven phone calls, and one for signaling data.

Organization of the project

The rest of the document is organized as follows. In Chapter 2, review the related reference paper as literature survey. In Chapter 3, system specification can be illustrated by ns2. In Chapter 4, the system architecture design and concepts are explained. In Chapter 5, the system organization can be explained with LRPH algorithm. In Chapter 6, implementation and results are explained. Finally, conclude this paper in Chapter 7.

For example Multi class (MC) is a position-aided routing protocol for power Heterogeneous MANETs. MC is to separate the whole routing area into cells and to select a high power node in each cell as the backbone node (B-node).MC achieves better performance with MAC protocol and the network layers to minimize the problems caused by link asymmetry. Hierarchical optimized link state routing (HOLSR) is a routing protocol somewhere the mobile nodes are controlled into clusters based on its capacity of a node. In a cross layer designed Device Energy-Load Aware Relaying (DELAR) framework that achieves energy conservation from multiple facets such as power attentive routing, broadcast preparation and power control.

Loose-Virtual-Clustering- routing protocol (LRPH) for Power Heterogeneous MANETs

(LRPH) and this protocol are used to exploits the benefits of the high power nodes where the unidirectional links are effectively detected. Clustering is the method for improving the network performance. In existing system, the strong coupling cluster is used. But it increases the cost of cluster construction and maintenance. Cluster is the efficient way for organizing the mobile nodes and it simplifies the heterogeneous mobile ad hoc network.

Heterogeneous mobile ad hoc network has the several different characteristics such as power, connection links (asymmetric links), signal, fluctuations, and etc. It needs the compatibility among the dissimilar standards. For example, IEEE 802.11 and other standards are interfaced by some portal address and it can be functional in the distribution system.

In LRPH, loose coupling can be established and this routing protocol used to avoid packet forwarding via high power nodes. The LVC algorithm used to find the unidirectional links and asymmetric links. Here, make the clusters for the mobile ad hoc networks and to establish the bidirectional links. LRPH also consists of route discovery and route protection. It conducted the analysis, simulation to

substantiate the effectiveness of LRPH in Microsoft WinCE environment.

CONCLUSION

Developed the new routing protocol named LRPH for power heterogeneous MANETs. LRPH is considered to be a double-edged sword because of its high-power nodes. To design an MEC algorithm to eliminate unidirectional links and to benefits from high-power nodes in transmission range, processing capability, reliability, and bandwidth. To develop the routing schemes to optimize packet forwarding by avoiding data packet forwarding through high- power nodes. Hence, the channel space utilization and network throughput can be largely improved. Through a combination of analytical modeling and an extensive set of simulations, to demonstrated the effectiveness of LRPH over power heterogeneous MANETs. The throughput of power heterogeneous MANETs can be impacted by high-power nodes and to construct the hierarchical network and to eliminate unidirectional links and reduce the interference raise by the high-power nodes.

Here to handle together the unidirectional links and asymmetric links. Next, use the high power node for rerouting the data and establish the bidirectional links. It can be improve the throughput of the mobile ad hoc network. In future, to research about the link residual time with the combination of both the bidirectional links and estimation of link duration and to improve the performance of power heterogeneous mobile ad hoc network.

REFERENCES

[1] Bhandari and N. Vaidya (Jan. 2008), "Heterogeneous multi-channel wireless networks: Routing and link layer protocols," AC M S IGMOBILE Mobile Comput. C ommun. Rev., vol. 12, no. 1, pp. 43–45.

[2] Cheng and J. Cao (2008), "A design framework and taxonomy for hybrid routing protocols in mobile ad hoc networks," Commun. Surveys Tu ts., vol. 10, no. 3, pp. 62–73, Third Quart.

[3] Du, D. Wu, W. Liu, and Y. Fang, (Jan. 2006), "Multiclass routing and medium access control for heterogeneous mobile ad hoc networks," IEEE Trans. Veh. Technol., vol. 55, no. 1, pp. 270–277, 77.

[4] Ghaderi, L. Xie, and X. Shen, (Aug. 2009), "Hierarchical cooperation in ad hoc networks: Optimal clustering and achievable throughput," IEEE Trans. Inf. Theory , vol. 55, no. 8, pp. 3425–3436.

[5] Huang, M. Y. Hsieh, H. C. Chao, S. H. Hung, and J. H. Park, (May 2009), "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks," IEEE J. Sel. Areas C ommun., vol. 27, no. 4, pp. 400–411.

[6] Huang, X. Yang, S. Yang, W. Yu, and X. Fu (Mar. 2011), "A cross-layer approach handling link asymmetry for wireless mesh access networks," IEEE Trans. Veh. Technol. , vol. 60, no. 3, pp. 1045–1058.

[7] Jeng and R.-H. Jan, (Dec. 2011), "Adaptive topology control for mobile ad hoc networks," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 12, pp. 1953– 1960.

[8] Lai, P. Lin, W. Liao, and C.-M. Chen,(Jan. 2011),"A region-based clustering mechanism for channel access in vehicular ad hoc networks," IEEE J. Sel. Areas C ommun., vol. 29, no. 1, pp. 83–93.

[9] Leonardi, E. Garetto, and M. Giaccone (Oct. 2009), "Capacity scaling in ad hoc networks with heterogeneous mobile nodes: The super-critical regime," IEEE/AC M Trans. N etw. , vol. 17, no. 5, pp. 1522–1535.

[10] Liu, X. Jiang, H. Nishiyama, and N. Kato, (Mar. 2012),"Exact throughput capacity under power control in mobile ad hoc networks," in Proc. 31th I EEE INFOCOM, pp. 1–9.

[11] Liu, C. Zhang, G. Yao, and Y. Fang (Sep. 2011), "Delar: A device–energy–load aware relaying framework for heterogeneous mobile ad hoc networks eous networks," IEEE J. Sel. Areas C ommun., vol. 29, no. 8, pp. 1572–1584.

[12] Ma and A. Jamalipour, "Opportunistic virtual backbone construction in intermittently connected mobile ad hoc networks," in Proc. I EEE ICC , Kyoto, Japan, Jun. 2011, pp. 1–5.

[13] Marina and S. R. Das,(Jun 2002),"Routing performance in the presence of unidirectional links in multihop wireless networks," in Proc. ACM MobiHoc, Lausanne, Switzerland, pp. 12–23.

[14] Shah, E. Gelal, and P. Krishnamurthy (Jul. 2007), "Handling asymmetry in power heterogeneous ad hoc networks," J. Comput. N etw.—Int. J. Comput. Telecommun. Netw., vol. 51, no. 10, pp. 2594–2615.

[15] Villasenor-Gonzalez, Y. Ge, and L. Lament, (Jul. 2005), "HOLSR: A hierarchical proactive routing mechanism for mobile ad hoc networks," IEEE Commun. Mag., vol. 43, no. 7, pp. 118–125.

[16] Wu and F. Dai (Sep. 2006),"Virtual backbone construction in MANETs using adjustable transmission ranges," IEEE Trans. M obile Comput. ,vol.5, no. 9, pp. 1188–1200.

[17] Xiang, X. Wang, and Y. Yang, "Supporting efficient and scalable multicasting over mobile ad hoc networks," IEEE Trans. M obile Comput. , vol. 10, no. 4, pp. 544–559, Apr. 2011.

[18] Yang, X. Yang, and H. Yang, (Oct. 2009), "A cross-layer framework for position based routing and medium access control in heterogeneous mobile ad hoc networks," Telecommun. Syst., vol. 42, no. 1/2, pp. 29–46.

[19] Yu and P. H. J. Chong, (2005), "A survey of clustering schemes for mobile ad hoc networks," Commun. Surveys Tu ts., vol. 7, no. 1, pp. 32–48, First Quart.

[20] Zhang, Q. Gao, J. Zhang, and G. Wang, (Sep. 2008), "Impact of transmit power on throughput performance in wireless ad hoc networks with variable rate control," Comput. C ommun., vol. 31, no. 15, pp. 3638–3642.