ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

Survey Paper on MANET's

Rajkumar L. Biradar

Department of Electronics & Telematics, G.Narayanamma Institute of Tech & Science, Hyderabad, India

ABSTRACT: MOBILE ad hoc networks (MANETs) have received increasing attention in recent years due to their mobility feature, dynamic topology, and ease of deployment. It 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 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.

KEYWORDS: MANETS, voting, nonvoting, node, security, static, dynamic network.

I. INTRODUCTION

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. 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.

Each of the nodes has a wireless interface to communicate with each other. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations. Device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. Due to nodal mobility, the network topology may change rapidly and unpredictably over time. The network is decentralized, where network organization and message delivery must be executed by the nodes themselves. Message routing is a problem in a decentralize environment where the topology fluctuates.

While the shortest path from a source to a destination based on a given cost function in a static network is usually the optimal route, this concept is difficult to extend in MANET. The set of applications for MANETs is diverse, ranging from large- scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. Because of these vulnerabilities, MANET is more prone to malicious attacks. A MANET is a most promising and rapidly growing technology which is based on a self-organized and rapidly deployed network. Due to its great features, MANET attracts different real world application areas where the networks topology changes very quickly. In many researchers are trying to remove main weaknesses of MANET such as limited bandwidth, battery power, computational power, and security.

II. VARIOUS PAPERS ON MANETS

In [2] authors used average residual battery level of the entire network and it was calculated by adding two fields to the RREQ packet header of a on-demand routing algorithm i) average residual battery energy of the nodes on the path ii) number of hops that the RREQ packet has passed through. According to their equation retransmission time is proportional to residual battery energy. Those nodes having more battery energy than the average energy will be selected because its retransmission time will be less. Small hop count is selected at the stage when most of the nodes have same retransmission time. Individual battery power of a node is considered as a metric to prolong the network lifetime in [3]. Authors used an optimization function which considers nature of the packet, size of the packet and distance between the nodes, number of hops and transmission time are also considered for optimization. In [4] initial population for Genetic Algorithm has been computed from the multicast group which has a set of paths from source to destination and the calculated lifetime of each path. Lifetime of the path is used as a fitness function. Fitness function will select the highest chromosomes which is having highest lifetime. Cross over and mutation operators are used to enhance the selection.

In [5] authors improved AODV protocol by implementing a balanced energy consumption idea into route discovery process. RREQ message will be forwarded when the nodes have sufficient amount of energy to transmit the message otherwise message will be dropped. This condition will be checked with threshold value which is dynamically changing. It allows a node with over used battery to refuse to route the traffic in order to prolong the network life. In [6] Authors had modified the route table of AODV adding power factor field. Only active nodes can take part in rout selection and remaining nodes can be idle. The lifetime of a node is calculated and transmitted along with Hello packets. In [7] authors considered the individual battery power of the node and number of hops, as the large number of hops will help in reducing the range of the transmission power. Route discovery has been done in the same way as being done in on-demand routing algorithms. After packet has been reached to the destination, destination will wait for time δt and collects all the packets. After time δt it calls the optimization function to select the path and send RREP. Optimization function uses the individual node's battery energy; if node is having low energy level then optimization function will not use that node. In 1999 Lidong Zhou and Zygmunt J. Haas [23], proposed Secure routing in networks such as the Internet has been extensively studied. Many proposed approaches are also applicable to secure routing in ad hoc networks. To deal with external attacks, standard schemes such as digital signatures to protect information authenticity and integrity have been considered.

The main advantage is secure key management service in an ad hoc networking environment and Signal strength monitoring. The disadvantage is normal operating system software indications seen when connected in infrastructure mode are unavailable in ad hoc mode. In 2004, Hao Yang and Haiyun Luo [10] proposed a new protocol to thwart threats. The existing proposals are typically Attack-oriented in that they first identify several security threats and then enhance the existing protocol. Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks.

The main advantage is we can protect the multi-hop network connectivity between mobile nodes in a MANET. Security issues are overcomed, many different types of challenges are proposed for secure designing that protect the MANET.

In 2005, Haowen Chan and Virgil D. Gligor [11] proposed an overview of key-distribution methods in sensor networks and their salient features to provide context for understanding key and node revocation. These techniques address only the key-establishment part of our key management problem. A set of high-level properties for distributed sensor-node revocation and a protocol is presented in the context of the Random Pair wise Key Distribution. Distributed revocation protocols have several advantages over centralized revocation. In 2006, Hao Yang and James Shu [13] proposed a unified network-layer security solution for such networks that protect both, routing and data forwarding operations through the same reactive approach. These protocols take the proactive approach and prevent malicious attacks by protecting the routing messages through cryptographic primitives. Exploits localized collaboration to detect and react to security threats. In this a self-organized public-key infrastructure for ad hoc networks is done, the idea is quite similar to pretty good privacy.

In 2007, Bounpadith Kannhavong and Nei Kato [5] proposed the current state of-the-art of routing attacks and counter measures in a MANET. We examine the routing attacks, such as link spoofing and colluding misrelay attacks, as well as we also consider the counter measures against such attacks in existing MANET protocols. The main advantage is Routing attacks are minimized in MANETS.

Although many solutions have been proposed, they still are not perfect in terms of tradeoffs between effectiveness and efficiency. Furthermore, each proposed solution can work only with a specific attack and we cannot consider all attacks at same time and is still vulnerable to unexpected attacks.

In 2009, Hide hisa Nakayama and Yoshiaki Nemoto [14] proposed a new dynamic anomaly detection system for MANETs. This scheme is based on a dynamic learning process that allows the training data to be updated. For enhancing the security in MANETs, which are vulnerable to attacks, robust learning methods against these attacks are required. The main advantage is effective performance against five simulated attacks and improves the accuracy of the overall system. The disadvantage is that various routing protocols have to be considered.

In 2007, Nidal Nasser and Yunfeng Chen [25] proposed the intrusion detection system ExWatchdog, its ability is to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. ExWatchdog solves a fatal problem of Watchdog. The use Throughput and Overhead as metrics to evaluate the performance of ExWatchdog. The main advantage is in decrease the overhead greatly, though it does not increase the throughput and it is not reliable.

In 2010, Kyul Park and Hiroki Nishiyama [22] proposed a certificate revocation scheme which takes into account of the reliability of each node, and accordingly constructs clusters to detect false accusations. We focus on the certificate revocation methods used in the certification system for MANETs, to cope with the wrong revocation of the certificate of legitimate users caused by false accusations by malicious nodes. The main advantage is it removes attackers from the network. The disadvantage is increase in the number of malicious nodes results in a increase in the amount of control traffic.

In 2004, James Parker and John Pinkston [15] proposed Network intrusion detection mechanism that relies upon packet snooping to detect aberrant behavior in MANETS. The main advantage is the dropping of the packet can easily be recognized and logged. The implementation of both the Passive and Active ID algorithms in GLOMOSIM led to a number of parameters that can be adjusted. The disadvantage is the performance is not greatly enhanced and the node density is not determined.

In 2005, Jean-Pierre Hubaux and Patrick T.Eugster [16] proposed the designing of certification authority in adhoc networks is done. A joint authority approach combines an offline identification authority and an online distributed revocation authority. The main advantage is it provides flexible certificate management protocols and a good trade overhead for robustness against various attacks. The disadvantage is that the node speed. As the node speed increases, this node speed weakens the tolerance of DICTATE to such attacks.

Various kinds of certificate revocation techniques have been proposed to enhance network security in the literature. In this, we briefly introduce the existing approaches for certificate revocation which are classified into two categories in Mobile Adhoc Networks.

The two categories are as follows.

1. Voting-Based Technique.
2. Non-Voting-Based Technique.

These existing techniques play a crucial role in our Mobile Adhoc Networks, which are discussed in detail in the following sections.

III. VOTING-BASED MECHANISM

Voting-based mechanism is defined as the means of revoking a malicious attacker’s certificate through votes from valid neighbouring nodes. URSA 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 neighbours. In URSA, each node performs one-hop monitoring, and exchanges monitoring information with its neighbouring 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 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 trust worthiness 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.

Routing and Packet Mechanism

The emerging mobile ad-hoc networking technology seeks to provide users “anytime” and “anywhere” services in a potentially large infrastructure less wireless network, based on the collaboration among individual network nodes. The growing civilian and military interest in these networks has made the access control service increasingly important. Restricting network access of routing and packet forwarding to well-behaving nodes, and denying access from misbehaving nodes are critical for the proper functioning of a mobile ad-hoc network where cooperation among all networking nodes is usually assumed. However, the lack of a network infrastructure, the dynamics of the network topology and node membership, and the potential attacks from inside the network by malicious and/or non-cooperative selfish nodes make the conventional network access control mechanisms not applicable.

Access control for mobile ad-hoc networks is challenging for several reasons. First, unlike a wired or wireless cellular network where access control mechanisms can be deployed at the access routers or base stations, an ad-hoc network is infrastructure-less and does not possess a well-defined, clear line of defense. Access control in an ad-hoc environment is a distributed problem by its nature.

Second, mobile users may roam freely in a potentially large network, and they demand “anytime, anywhere” ubiquitous services. It is desirable that any services for access control be available at each networking node’s locality, in order to avoid communication over highly unreliable, multi-hop wireless channels.

Third, the solution has to handle misbehaviors by selfish and malicious nodes from inside the network. These misbehaving insiders may already possess certain information on the access control.

One of the existing approach (COCA) deals with misbehavior prevention [37] in mobile ad-hoc network. In which, every mobile node can be issued a ticket by these servers to participate in networking activities. However, in order to effectively identify and isolate malicious nodes and selfish nodes, these tickets have to be periodically renewed or certain ticket revocation service has to be maintained at these servers. In either case, heavy communication with these servers is involved, which may stress the mobile ad-hoc network due to the bandwidth limit of the wireless link and the multi-hop routing failures caused by node mobility.

Ticket Mechanism

In a mobile ad-hoc network that is protected by URSA, each networking node is required to carry a valid ticket in order to participate in network activities. A ticket is considered valid if it is certified and unexpired. When an existing node moves to a new location, or a new node joins the network, it exchanges tickets with its one-hop neighboring nodes to establish mutual trust relationship.

Misbehaving nodes without valid tickets will be denied from all networking activities, therefore isolated from the mobile ad-hoc network. URSA [12] ticket services ensure that ideally only well-behaving nodes receive tickets. The implementation of ticket renewal and revocation services is fully distributed into each well- behaving node through an initialization process during the bootstrapping phase of the network.

Ticket Format

For nodes that join or rejoin the network, they can be initialized by a certain number of neighbors in order to serve other nodes for ticket renewal and revocation. Neighboring nodes also monitor each other during the normal operations with certain misbehavior detection mechanisms of their choice. When its ticket is about to expire, a node will itself solicits to its neighboring nodes to collectively renew its own ticket.

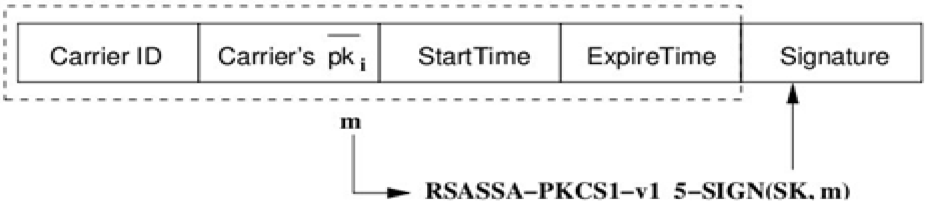

Figure: 2.3 Ticket Format

A neighboring node responds to such request only if the requesting node is considered as being well behaving during the last monitoring period. Furthermore, an accusation message will be flooded locally once a misbehaving node is detected by any of its neighboring nodes. Misbehaving nodes, once detected and convicted, will not be able to have their tickets renewed. An URSA ticket serves as a passport for a networking node. It provides a simple, yet effective mechanism for controlling the access from well-behaving and misbehaving nodes. A typical URSA ticket1 is shown in figure. It includes the ID of the ticket carrier; the ticket carrier's personal pki, and the Start Time and Expiration Time, and a Signature on the message digest of the ticket body. The node ID can be its IP address, or its MAC address in the context of an ad-hoc networking environment. The ticket binds the Carrier's ID and its personal public key pki that is usually used to establish secure communication channels.

Start Time and Expiration Time define the ticket validity period Tcert. The Signature verifies the message integrity, and is generated using a system RSA secret key (SK, N)2 . A ticket can be verified by applying the well-known, system public key (P K, N) on the ticket Signature. No single node in the network has complete information of the exponent SK of the system secret key (SK, N) that is used to sign tickets. Instead, each node with ID vi holds a share Pvi as partial information of SK. Tickets identify well-behaving nodes. When a mobile node moves to a new location, it exchanges tickets with its new neighbors, as the first step to cross-verify each other. Tickets are stamped with expiration time.

Localized Ticket Renewal

The localized ticket renewal figure is shown as follows. Nodes have to be issued a new ticket upon the expiration of its old ticket. Our goal is to localize [20] this service into each node's neighborhood in order to maximize service availability and resilience against potential attacks, while conserving network resources and system scalability by localizing the communication traffic.

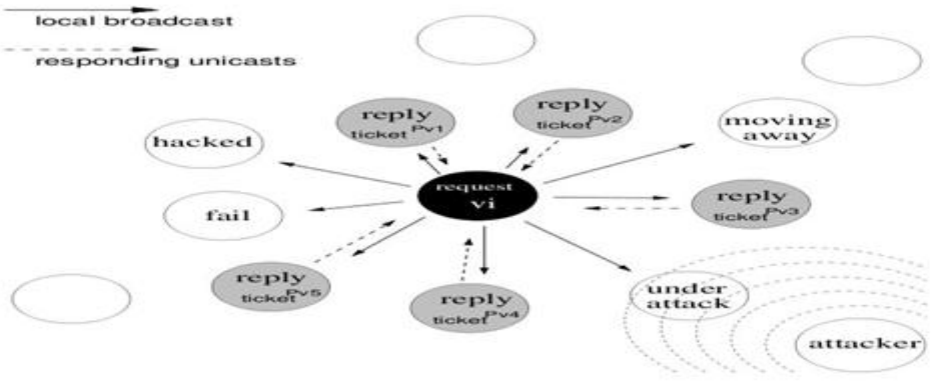

Figure: 2.4 Localized Ticket Renewal

Disadvantages of voting-based mechanism

Following are disadvantages of voting-based schemes:

1. Susceptibility to false accusations: Attacker-controlled nodes can transmit votes against legitimate nodes without consequence. This undermines the credibility of votes from honest nodes.
2. Susceptibility to Collusive attackers: Attacker-controlled nodes can concentrate themselves in a chosen location to create a local majority.
3. Susceptibility to Sybil and replication attacks Attacker-controlled nodes [3] can rig votes with spurious identities or by re-using an identity in multiple locations.
4. Susceptibility to selective misbehavior, threshold voting schemes is vulnerable to an attacker who reveals detectable misbehavior to just fewer nodes than the number needed to initiate revocation.
5. Slow attack response since no single node’s claim can be trusted, significant time may pass, and attacks may be launched, before a voting scheme triggers a revocation order.
6. High storage and communications overhead Threshold voting and reputation systems impose significant storage and computational requirements.

Reaching decisions can be made much simpler if we allow a single node to decide. If a node believes another has misbehaved, then it can carry out punishment. The trouble with this approach is that a malicious node can falsely accuse legitimate ones; the solution is to make the act of punishment costly. We propose a simple, albeit radical strategy: suicide for the common good. Upon detecting a node M engaging in some illegal activity, A broadcasts a signed suicide note which includes the identities of both A and M. The other nodes in the network then verify the signature and, if correct, revoke both A and M. This can be achieved by adding both identities to a blacklist and deleting all keys shared with either node. This strategy is premised on the observation that if a node determines another node has cheated, there is no more convincing way to let its neighbors know of its sincerity than to transmit a signed self-revocation certificate.

IV. NON-VOTING-BASED MECHANISM

In the non-voting-based mechanism we don’t consider the votes of the neighboring nodes. This non-voting based is entirely opposite to the voting based mechanism. In a self-organized system, by contrast, no clear, universally accepted authority exists, so the revocation process becomes much more difficult (and costly) to implement in practice. This is because it is unclear how to decide whether a device should be revoked. A malicious participant can falsely accuse another node of misbehavior. Even if a decision can be reached, revoking credentials [26] remains challenging since nodes do not necessarily trust claimed results from the vote.

The proposed a radical strategy, suicide for the common good, which drastically simplifies the decision making process and revocation orders. It allows a single node to revoke a malicious node from the network at the cost of its own membership. This strategy mimics a number of mechanisms prevalent in nature, such as the sacrificial action of bees defending the hive by stinging an intruder and dying as a result. The immediate goal is not to describe a fixed protocol but to present and analyze this new strategy, highlighting the necessary conditions to make it viable.

The revocation proposal exhibits a number of desirable properties: it is fully decentralized, incurs low communication and storage overhead, enables fast removal of misbehaving nodes, and is ideally suited to highly mobile networks. Yet collective decision-making is slow, expensive and prone to manipulation. Suicide for the common good exhibits several appealing properties compared to other decision-making schemes. The decision making schemes at some instances may not be that appropriate when compared to our properties. We consider both of them separately. In this totally we have six different properties. These six different properties play a crucial role in our mechanism. Each and every property is explained in a very detailed manner in our mechanism.

The six different properties are as follows.

1. Fully decentralized so need to consult a base station.
2. Very fast removal therefore delays occur while waiting on votes or thresholds to be met.
3. Unconstrained node mobility nodes are not restricted to a location or set of voting neighbors.
4. Undermines false claims as attack strategy false claims remove only one innocent node.
5. Single node detection only one honest node has to detect misbehavior to initiate revocation.
6. Low communications overhead hence, no need to send messages back and forth between voting members.

We note that suicide for the common good is an effective decision-making strategy only when certain conditions are met:

1. Attacker benefit from removing one innocent node must be less than the benefit of having a malicious node placed inside the network.
2. Honest nodes share common interest.
3. An absence of unforgettable, independently verifiable and conclusive proof.
4. Low likelihood of two good nodes accusing each other.
5. Difficult to prevent malicious nodes from issuing false claims.

Condition 1 can be met whenever the number of good nodes dominates the number of bad nodes present in the system. In addition, the value of nodes must be consistent: a smart dust mote must not be able to revoke a base station, for instance. When the condition is met, we can afford to sacrifice a good node for the benefit of removing a bad node. This is a strategy employed in nature (e.g., white blood cells in macrophage). The suicide scheme could be extended to more general ratios reflecting the relative value of nodes (e.g., requiring two nodes to be sacrificed in order to remove one bad node).

One threat is that adversaries may use a node's removal to disrupt a valid route or create a numerical advantage in an area. In principle, the adversary should not be able to influence network topology. To mitigate this threat, we propose that reinforcements be sent to repopulate an attacked area. This is a natural response since a series of suicides in a region indicates likely enemy action [19]. Thus we can probabilistically move nodes closer to the area where the suicide note has been issued.

Condition 2 requires honest nodes to value the social welfare of the network over individual utility. This condition is reasonable whenever the nodes are deployed by a single entity (e.g., a sensor network deployed on a battlefield) as opposed to when nodes are individually controlled (e.g., a peer-to-peer file-sharing system).
While conditions 1 & 2 are system dependent, conditions 3–5 depend on the corresponding detection mechanism.

Hence the detection mechanism impacts the choice of the most appropriate revocation strategy. Occasionally, evidence of misbehavior is non-repudiable to any third party, which normally requires digital signatures and asymmetric cryptography. Detection mechanisms producing universally verifiable evidence include geographic packet leashes for detecting wormholes and node replication detection in sensor networks.

For these schemes, suicide for the common good is inappropriate, since the malicious node's guilt is incontrovertible and verifiable to all without the need for consensus (contradicting condition 3). However, generating universally non repudiable evidence can be costly, implicitly requiring widespread use of public key cryptography and broadcasting many signed messages. Furthermore, situations where a malicious node is forced into self-incrimination are limited. This excludes, for in- stance, detecting a malicious node that chooses to not do something such as dropping a message. More commonly, detection mechanisms create evidence that is non-repudiable only to a single party. This can happen for evidence signed using a pair-wise unique symmetric key, for instance.

A message authentication code guarantees origin authenticity to the nodes who hold the signing key. If pair-wise symmetric keys are used, then the two nodes sharing the key know the message is authentic; however, no other nodes are so assured. Detection mechanisms of this type include temporal packet leashes, Sybil attack detection by querying for possessed keys and distance-bounding protocols. Such detection mechanisms are amenable to suicide. Malicious nodes cannot trick honest nodes into falsely accusing each other without knowing the relevant key. Yet dishonest nodes can easily levy false accusations because evidence is not universally verifiable. 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.

V. DRAWBACKS OF EXISTING TECHNIQUES

Comparing the disadvantages in the both existing techniques namely, voting based technique and non-voting based technique. The disadvantage of the voting based technique is as follows. In the voting based technique the decision processes to satisfy the condition of certificate revocation is, however, slow. Also, it incurs heavy communications overhead to exchange the accusation information for each other.

The disadvantage of the non-voting based technique is as follows. In non-voting based technique the accuracy of determining an accused node as a malicious attacker and the reliability of certificate revocation will be degraded when compared with the voting-based method. The former achieves higher accuracy while judging a suspicious node, but takes a very longer time than the latter can significantly expedite the revocation process.

VI. Conclusion and Future Work

A major issue is to ensure a secure communications in MANET, certificate revocation of attacker nodes is addressed. Cluster-based certificate revocation with vindication capability scheme has advantages of both voting-based and non-voting based mechanisms in which malicious certificate is revoked and false accusation problems are solved. This CCRVC scheme reduces the revocation time as compared to the voting-based mechanism.

In the cluster based model falsely accused nodes are restored by the CH, which improves the accuracy when compared to the non-voting based mechanism. The legitimate nodes are released and restored in a new stimulant method which also enhances the number of available normal nodes in the network for protecting the efficiency of quick revocation.

References

1. A.M. Hegland, E. Winjum, C. Rong, and P. Spilling, “A Survey of Key Management in Ad Hoc Networks,” IEEE Communications” Surveys and Tutorials, vol. 8, no. 3, pp. 48-66, Third Quarter 2006.
2. Adnan Nadeem, Member, IEEE, and Michael P. Howarth “A Survey of MANET Intrusion Detection & Prevention Approach or Network Layer Attacks”, IEEE Trans. Mobile Computing, vol. 5, no. 6, pp. 364-374, Sept-Oct. 2009.
3. Amara korba, Abdelaziz, Mehdi Nafaa, GhanemiSalim: “Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks”., IEEE Journal on Selected Areas in Communications, Vol. 21, no. 4, pp.368-379.
4. A.Rangaswamy and H.K.Pung, “Enhancement of passive cluster based routing for mobile adhoc networks,” in Eleventh International Conference on Computer Communications and Networks, October 2002,pp. 376-381.
5. Bounpadith Kannhavong, H. Nakayama, A. Jamalipour, Y. Nemoto, and N.Kato, “A Survey of Routing Attacks in MANET,” IEEE Wireless Communications. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007.
6. C. Bettstetter, G. Resta, and P. Santi, “The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad Hoc Networks,” IEEE Trans. Mobile Computing, vol. 2, no. 3, pp. 257-269, July-Sept. 2003.
7. C. Gentry, “Certificate-Based Encryption and the Certificate Revocation Problem,” EUROCRYPT: Proc. 22nd Int’l Conf. Theory and Applications of Cryptographic Techniques, pp. 272-293, 2003.
8. Dang Nguyen, Pascale Minet, Thomas Kunz and Louise Lamont: “On the Selection of Cluster Heads in MANETs”. IEEE Journal on Selected Areas in Communications,” Vol. 2, no.5, pp.326-339.
9. Garth V. Crosby, NikiPissinou, James Gadze **“**A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks”. Wireless Comm. and Mobile Computing (WCMC) Special Issue on Mobile Ad Hoc Networking” Research, Trends, and Applications, vol. 5, no.3, pp. 511-521, 2009.
10. Hao Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in Mobile Ad Hoc Networks: Challenges and Solutions,” IEEE Wireless Communications”, vol. 11, no. 1, pp. 38-47, Feb. 2004.
11. H. Chan, V. Gligor, A. Perrig, and G. Muralidharan, “On the Distribution and Revocation of Cryptographic Keys in Sensor Networks,” IEEE Transactions Dependable and Secure Computing, vol. 2, no. 3, pp. 233-247, July 2005.
12. [12] 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.
13. H. Yang, James Shu, X. Meng, and S. Lu, “SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks,” IEEE J. Selected Areas in Communications., vol. 24, no. 2, pp. 261-273, Feb. 2006.
14. H. Nakayama, S. Kurosawa, A. Jamalipour, “A Dynamic Anomaly Detection Scheme for Aodv-Based Mobile Ad Hoc Networks,” IEEE Transactions Vehicular Technology, vol. 58, no. 5, pp. 2471-2481, June 2009.
15. James Parker and John Pinkston “On Intrusion Detection and Response for MANETS” “Proc. Sixth ACM Int”l Symp. Mobile Adhoc Networking and Computing,” pp. 254-265, 2004.
16. Jean-Pierre Hubaux, and Patrick T. Eugster “DICTATE: Distributed Certification Authority with Probabilistic freshness for Ad Hoc Networks,” IEEE Transactions. On Dependable And Secure Computing, Vol. 2, No. 4, October-December 2005.
17. Jie Wu, Fei Dai, “Broadcasting in Ad Hoc Networks: Based on Self-Pruning”, Twenty Second Annual Joint Conferences of IEEE Computer and Communication Societies, IEEE INFOCOM 2003
18. J. Lian, K. Naik, and G.B. Agnew, “A Framework for Evaluating the Performance of Cluster Algorithms for Hierarchical Networks”, IEEE/ ACM Transactions. Networking, vol. 15, no. 6, pp. 1478-1489, Dec. 2007.
19. J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil Routing Attacks in the Network: Analysis & Defenses,” Proc. Third Int’l Symp. Information Processing in Networks, pp. 259-268, 2004.