International Journal of Security and Its Applications
Vol. 10, No. 1 (2016), pp.287-302
http://dx.doi.org/10.14257/ijsia.2016.10.1.27

A Lightweight Certificate Revocation Scheme for Hybrid Mobile ad Hoc Networks

Huaqiang Xu[1, 2], Rui Wang[2] and Zhiping Jia[2*]

[1]*School of Physics and Electronics, Shandong Normal University*
[2]*School of Computer Science and Technology, Shandong University*
[1]*xuhuaqiang12@163.com*

Abstract

Hybrid mobile ad hoc networks have received increasing attentions due to some attractive features. However, these features such as wireless communication and dynamic topology make it face more challenges in providing secure network services. This paper focuses on the certificate revocation issue which is an important component of certificate management. The existing certificate revocation schemes for mobile ad hoc network either consume more time and accusation overhead to revoke a certificate or need to be improved in terms of revocation accuracy. In this paper, we propose a lightweight certificate revocation scheme for hybrid mobile ad hoc network to achieve a performance trade-off between efficiency and reliability. In particular, to improve the efficiency, the scheme revokes certificate when the accusation weight of the accuser is larger than the accused node; to guarantee the reliability, the revoked nodes are evaluated again by wrong revocation recovery mechanism, so the wrongly revoked nodes will be detected and recovered. Simulation results demonstrate the proposed scheme can achieve a performance trade-off between high accuracy obtained by voting-based scheme and other performance metrics like short revocation time and low overhead obtained by non-voting-based scheme.

Keywords*: certificate revocation, mobile ad hoc network, security, performance trade-off*

1. Introduction

In recent years, mobile ad hoc networks (MANETs) have attracted increasing attentions due to their self-organizing nature and ease of deployment. A MANET comprises a group of mobile nodes, which can communicate with other nodes located within the transmission range directly, or employ a multi-hop communication to reach non-neighboring nodes. Some works [1, 2] integrate MANETs with the Internet to extend the network coverage and enhance the flexibility of network. The so called hybrid MANET employs gateway nodes as bridge to translate the protocols between two heterogeneous networks.

The wireless and mobility nature make MANETs face more security risks than traditional wire networks [3, 4]. Thus, effective security mechanism is one crucial prerequisite for secure network communication. Lots of researches have been down to secure wireless networks, like the detection of attacks [5-7], various kinds of cryptographic algorithms [8-10] and security strategies with certificate management [11-14]. Among them, certificate management is a widely adopted mechanism which helps validate the trustworthiness of mobile nodes. Before joining a MANET, every

Zhiping Jia is thr Corresponding Author.

ISSN: 1738-9976 IJSIA

mobile node is issued a certificate. However, a node even with valid certificate may work maliciously and thus threaten the security of network. In this case, certificates of malicious nodes should be revoked. Therefore, certificate revocation is an important part of certificate management. Also because of this, tremendous amount of works [13-20] have been made for it. The existing certificate revocation approaches are mainly classified into two categories: voting-based mechanism and non-voting-based mechanism. The voting-based mechanism [15, 17, 21] revokes the certificate of the accused node when the weighted sum from voters exceeds a predefined threshold. Owing to more nodes are required to participate in the revocation process, this approach focuses on the accuracy and reliability, however suffers from high overhead and long revocation time. On the contrary, in the non-voting-based mechanism [13, 18-20], any single node with valid certificate can directly revoke a suspicious malicious node by making an accusation. However, this method suffers from low accuracy especially in the environment with false accusation.

This paper proposes a lightweight certificate revocation scheme for hybrid ad hoc networks. The scheme takes advantage of the voting-based mechanism by allowing several nodes to participate in the revocation process to ensure the reliability. Meanwhile, to expedite the revocation process, we propose an 'acceleration strategy' to reduce the number of voters needed to revoke a certificate, that is, once the weight of the accuser is larger than that of the accused node, the certificate of the accused node is revoked immediately. Furthermore, in order to enhance the accuracy, the scheme provides vindication capability to cope with wrong certificate revocation by allowing the one-hop neighboring nodes to recover the certificate of wrongly revoked node. If the number of recovery packets exceeds a predefined number, the wrongly revoked node will be removed from Certificate Revocation Lists (CRLs).

The remainder of this paper is organized as follows: Section 2 briefly overviews the related works on certificate revocation approach in MAENTs. In Section 3, the assumptions of the proposed scheme are given. In Section 4, we describe the proposed scheme in detail. Section 5 presents and analyses the simulation results using NS-2.33 network simulator. Finally, we conclude the paper.

2. Related Works

Recently, many certificate revocation mechanisms have been proposed for mobile ad hoc networks. The decision whether to revoke a node's certificate or not is made according to the observations and accusations from its one-hop neighboring nodes. According to the number of accusations needed in making decision, the existing approaches can be simply classified into two categories: non-voting-based mechanism and voting-based mechanism.

In the non-voting-based mechanism, the certificate of a node is revoked by only one accusation from any legitimate node. In [18], a 'suicide strategy' is adopted to revoke certificate, in which a node is recognized as a malicious node and revoked certificate by only one accusation. The approach is very efficient in terms of revocation time, however, at the cost of sacrifice of the accuser. That is, both the accuser and the accused node are revoked certificate and isolated from the network. Meanwhile, the false accusations made by malicious nodes degrade the accuracy of the approach.

Liu etc. [20] proposed a cluster-based certificate revocation approach with vindication capability (CCRVC). In this approach, the certificate of a suspicious node is revoked by only one accusation. The accuser is deprived of the accusation function instead of being isolated from the network and, its accusation function can be restored when the legitimacy of its accusation is affirmed by a threshold-based estimation mechanism. In order to improve the accuracy of the scheme, the cluster head is responsible for detecting the falsely accused nodes within its cluster and recovering their certificates. However, further secure mechanisms should be designed to ensure the reliability and trustworthiness of the

cluster head.

In the voting-based mechanism, the certificate revocation is the result of the vote of all neighboring nodes. In [21], a suspicious node is recognized as a malicious node only if there are at least m out of N mobile nodes cast accusations independently against it. This scheme achieves a higher accuracy of certificate revocation, however, requires a long time to revoke a certificate. Besides, the selection for the value of m is another challenge.

To improve the efficiency of certificate revocation, some schemes [15, 17] assign each node a value as accusation weight. The accusation weight, which indicates the trustworthiness of the node, is calculated according to the past behaviors, like the number of accusations made against other nodes and that accuse it from others. The node with higher accusation weight plays a more important role in the certificate revocation process. When the weighted sum of accusations against a suspicious node exceeds a predefined threshold, the certificate of the accused node is revoked. The voting-based mechanism enhances the accuracy of certificate revocation, owing to the participation of all nodes. However, the participation of all nodes increases the communication overhead, due to that more voting messages are exchanged between mobile nodes.

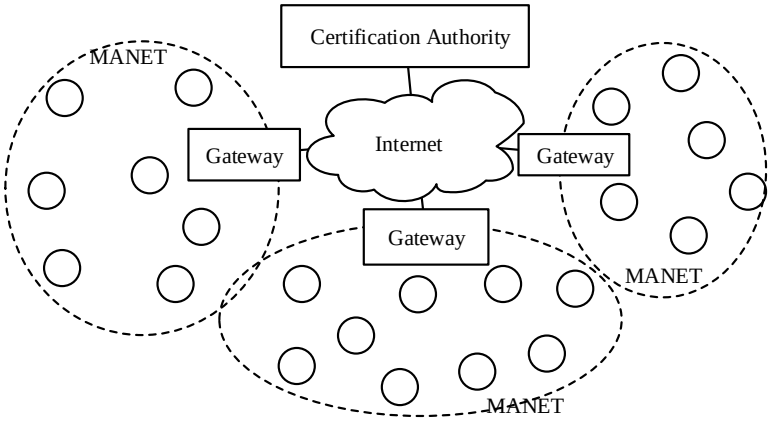

Figure 1. Network Architecture

3. Assumptions of the Scheme

In this section, we first introduce the model of the proposed revocation scheme for hybrid mobile ad hoc networks. We assume that there are several MANETs in the network, and mobile nodes can roam freely from a MANET to another one. Each MANET connects with the Internet through a gateway node, which works as a bridge between two heterogeneous networks. We assume that all gateway nodes are well protected and can be trusted. They are also equipped with more resource for calculation and data storage than ordinary mobile nodes. A trusted third party, certificate authority, is deployed in the network to manager all nodes' certificates, including certificate distribution and certificate revocation. Since only the issue of certificate revocation is discussed, the scheme assumes that every mobile node has already got a certificate when joining a MANET. To address the certificate revocation scheme, we assume that all nodes work in promiscuous mode. Thus, mobile nodes are able to detect malicious activities of their one-hop neighboring nodes by using various detection systems. However, the issue on attack detection mechanism is beyond the scope of this paper. We assume that all malicious activities can be detected. The architecture is illustrated in

Figure 1.

Once a node detects malicious activities of its one-hop neighboring node, it sends an accusation packet to the gateway node. Each node is allowed to accuse a given node only once. The gateway node is in charge of the execution of certificate revocation algorithm, including updating the variables of each mobile node, calculating the accusation weight, storing accusation packets and determining whether a node should be revoked or not. The accusation weight of a node is calculated according to its past activities, such as accusing other nodes or being accused by other nodes. Higher accusation weight means the node is more trusted as a legitimate node. Once the weight of the accuser is larger than that of the accused node, the certificate of the accused node is revoked. With this 'acceleration strategy', the proposed certificate revocation scheme can remove a misbehavior node more quickly than traditional threshold-based voting method. Besides, the malicious node can launch false accusation attacks against a legitimate node with a predefined attack probability. As a result, the certificate of a legitimate node may be wrongly revoked. To cope with wrong certificate revocation problem, mobile node is allowed to send vindication packets to the corresponding gateway node whenever it thinks the certificate of its one-hop neighboring node is wrongly revoked. The gateway node is in charge of the final decision.

4. Details of the Scheme

In this section, the details of the proposed certificate revocation scheme are given.

4.1. Data Collection

Mobile nodes accuse other nodes by sending accusation packets. The accusation packets are finally forwarded to the corresponding gateway node and stored in the accusation list for a period of time after they are processed. These accusations are used to calculate the accusation weight of nodes and estimate the legality of a suspicious node.

The proposed scheme needs to keep track of the following variables, the values of which are used to compute accusation weight:

A_i: The variable represents the total number of accusations made against node i. Both the accuser and the accused node should have valid certificates. When a gateway node receives a valid accusation packet, it updates this variable, and then stores the packet in its accusation list table. The initial value is set to zero.

a_i: It records the total number of accusations made by node i. The accuser is not allowed to accuse a same node twice. When the accusation made by node i is received by the gateway node, this variable will be updates. However, if the certificate of the accused node is finally revoked, the accusations made against it are not counted. The initial value is set to zero.

w_i: The value of this variable represents the accusation weight of node i. This variable, initialized as 1, is a real number between 0 and 1. It depends on the number of accusations both made by node i and against node i. The greater the value of w_i, the more trustworthy of node i. The value is calculated as follows:

$$w_i = 1 - \lambda A_i - \lambda a_i \quad , \qquad (1)$$

Where $\lambda = 1/2(N-1)$ and N is the number of the mobile nodes in a MANET. The value of λ keeps w_i be large than 0.

CS_i: This variable indicates the certificate status of node i. Three statuses are available as described below:

$$CS_i = \begin{cases} 1, & \text{the certificate is valid.} \\ 0, & \text{the certificate is under dispute.} \\ -1, & \text{the certificate is revoked.} \end{cases} \quad (2)$$

If the value of CS_i is -1, node i is isolated from network communication. If the value is 0, the scheme cannot determine the validity of node i. At such status, node i still has a certificate, however, is deprived of the ability to accuse other nodes.

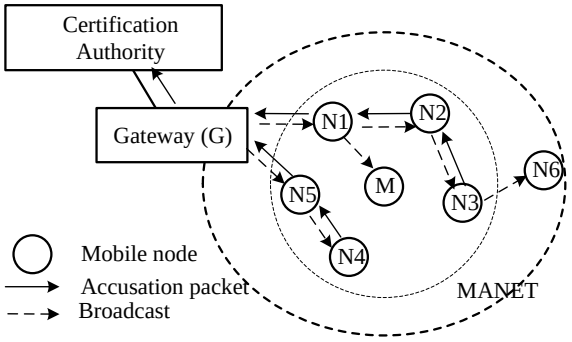

Figure 2. Revoking a Node's Certificate

4.2. Certificate Revocation Procedure

Each node is monitored by its one-hop neighbors, and malicious activities can be detected. The revocation procedure is started when attack activities of a node are detected. Every legitimate one-hop neighboring node checks whether the malicious node is listed in local CRL or not. If the certificate of malicious node has been revoked, nothing needs to be down. Otherwise, each neighboring node makes an Accusation Packet (AP) and sends it to the corresponding gateway node. Upon receiving the AP, the gateway node checks the status of accuser's certificate. If the certificate is valid, the AP will be stored in the accusation list, and the variables of both the accuser and the accused node are updated. If the weight of the accuser is larger than that of the accused node, the accused node will be recognized as a malicious node and added to the CRL of the gateway node. After that, the gateway node notifies CA to revoke the certificate of the accused node and meanwhile informs mobile nodes by broadcasting this revocation information to the MANET.

Take Figure 2 as an example. Malicious node M launches attacks towards some nodes and, its malicious activities are detected by one-hop neighboring nodes N1, N2, N3, N4 and N5. The scheme revokes M's certificate according to the following procedure:

Step 1. Each of neighboring nodes (N1, N2, N3, N4 and N5) detects malicious activities of node M and casts an accusation packet against node M. The accusation packets are forwarded to gateway G.

Step 2. All accusations are cached in the waiting list of gateway G. They are processed one by one according to their arriving time.

Step 3. If the waiting list is empty, go to Step 6. Otherwise, Gateway G processes the earliest arrived accusation, supposing made by node x. Gateway G updates a_x and A_m, stores the accusation in the accusation list, and calculates the accusation weight of node x and M. If w_x is larger than w_m, go to Step 4, otherwise, repeat Step 3.

Step 4. Gateway G clears all accusations in the waiting list; adds node M to the CRL; notifies the CA and broadcasts the revocation information to the MANET; updates a_i (minus one) for all nodes successfully accused M.

Step 5. Upon receiving the revocation information, mobile nodes update their local

CRL.

Step 6. Finish the procedure.

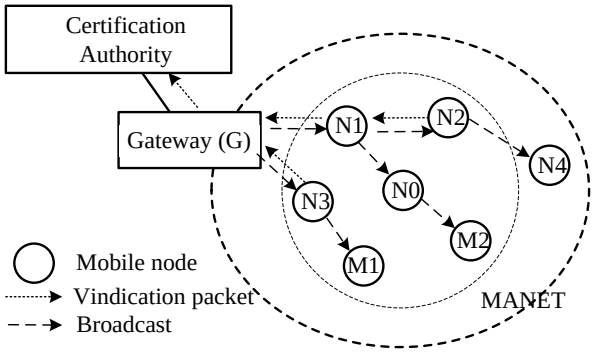

Figure 3. Recovering a Wrongly Revoked Node

4.3. Dealing with Wrong Revocation

False accusations made by malicious nodes against legitimate nodes influence the reliability of the scheme. In this subsection, we detail the methods to degrade the influence of false accusations. As described in Section 4.1, once a false accusation is accepted by the gateway node, the weight of the accused legitimate node will be reduced. This degrades the ability of the legitimate node to revoke the certificate of malicious node, and increases the risk for legitimate node to be wrongly revoked.

If a node is wrongly revoked, its one-hop neighboring nodes and the gateway node will cooperate to recover its certificate. As discussed in the above subsection, when a node is determined as a malicious node according to the accusation messages, gateway node will broadcast the decision to the MANET to inform all mobile nodes. Each node updates its local CRL to record the new certificate revocation information. However, if a node is falsely accused and wrongly revoked, all of its legitimate one-hop neighboring nodes can aware that the revocation decision is incorrect, for they have not detected any malicious activities since being its neighbors. Consequently, neighboring nodes try to correct the mistake by sending Vindication Packets (VPs) to the corresponding gateway node. When the gateway node receives VPs, recovery mechanism is started to re-estimate the validity of the node under dispute. If the number of VPs exceeds a predefined threshold K, the under dispute node is recognized as a legitimate node and recovered certificate.

For example, in Figure 3, node N0 is a legitimate node and is wrongly revoked due to the accusations made by malicious nodes M1 and M2. We suppose that the accusation made by M1 directly result in the wrong certificate revocation of N0. Nodes N1, N2, N3, M1 and M2 are one-hop neighbors of node N0. Certificate recovery procedure is described as bellowing:

Step 1. The certificate of node N0 is revoked. All mobile nodes are informed this certificate revocation.

Step 2. Legitimate nodes N1, N2, N3 detect that N0 was wrongly revoked. Thus, each of them sends a vindication packet to gateway G independently.

Step 3. Gateway G receives these vindication packets and counts the number of them. If the number is larger than the predefined threshold K, the certificate of N0 is recovered. Meanwhile, Gateway G updates the value of variables: A_{n0} --, a_{m1}++ , notifies CA and all mobile nodes the new decision. Otherwise, the status of N0 is set to 0.

Even if the recovery operation is not successful, the node N0 is still removed from the CRL and the status of which is set as under-dispute. This status deprives the right to accuse other nodes, however, still allows the node to take part in the communications. In

the future, if the node under-dispute is accused again, its certificate will be revoked directly. Besides, there are also other chances for an under-dispute node to be recovered. For example, if the node, which accusation directly results in the wrong certificate revocation, is affirmed as a malicious node, the under-dispute node will be revived.

4.4. Node Migration

In the proposed architecture, each gateway node is in charge of communication security for mobile nodes in a MANET. Thus, a gateway node only traces the activities of mobile nodes of its MANET. However, mobile nodes can roam freely from a MANET to another one. When a mobile node moves to another MANET, the corresponding gateway node should first verify the validity of certificate by querying the CA. The query result is broadcasted to the whole MANET. If the certificate of the new joining node is not listed in the certificate revocation list, the gateway node should further get its history activity information by communicating with the previous gateway node. This helps to track the overall activities of a node before evaluating its validity. Thus, this tracking mechanism is valuable for the reliability of certificate revocation scheme in the case of node migration.

4.5. Discussion

In order to reduce revocation time, our certificate revocation scheme do not adopt 'voting period' used in previous works [15]. In other words, whenever the accusation weight of the accuser is larger than that of the accused node, the certificate of the accused node is revoked immediately, not at the end of the voting period. When the legitimate nodes take the majority of the network, intuitively, this mechanism can work effectively. However, it is possible for a legitimate node to be wrongly revoked, even if there are only very few malicious nodes in the network. For example, supposing that only two malicious nodes M1, M2 exist in the network and both of them are the neighboring nodes of a legitimate node N. If M1, M2 both falsely accuse node N at the beginning, the accusation weight of M1 or M2 may larger than that of N, and this leads to the certificate revocation of N.

Therefore, the wrong revocation recovery mechanism is particularly important to ensure the accuracy of revocation scheme. The selection of threshold K is critical for the vindication of wrongly revoked nodes. Liu etc. [20] have proved by both the mathematical analysis and simulations that the optimal threshold K is equal to M/2, where M is the number of one-hop neighbors. The optimal threshold increases the accuracy of determining whether an accused node is a malicious node or a legitimate node, however, still cannot achieve one hundred percent accuracy. Because it is possible that more than half neighboring nodes of a given node are malicious nodes.

Table 1. Simulation Parameters

Parameter	Value
Simulation area	1000m×1000m
Transmission range	250m
Simulation time	600s
Mobility model	Random way point (RWP)
Pause time	10s
Gateway coordinate	(0, 500)
Maximum speed	10m/s
False accusation probability(p)	0.2 or 0.5

5. Performance Evaluation

In this section, we present and discuss the simulation results conducted in the network simulator, NS-2.33, which is extended with the Global Connectivity support [22]. We first run simulations to evaluate the performance of the proposed certificate revocation scheme, in particular, to affirm the effectiveness of the wrong revocation recovery mechanism. To verify that our proposed scheme achieves a performance trade-off between voting-based mechanism and non-voting-based mechanism, we design extensive simulations to compare the efficiency and reliability of different certificate revocation schemes.

5.1. Simulation Setup

In the simulation, mobile nodes, which construct a mobile ad hoc network, are placed randomly in a square flat space area (1000m × 1000m). A gateway node is placed in the center of any edge of the square to provide Internet services. Each mobile node has the fixed transmission range as 250 meters, moves following the random way-point mobility pattern [23], and communicates with other mobile nodes by running ad hoc on-demand distance vector (AODV) [24] as the routing protocol. The maximum velocity and the pause time are set to 10 m/s and 10 seconds, respectively. Among the mobile nodes, some are randomly designated as malicious nodes, which may launch false accusation attacks towards neighboring nodes with a predefined attack probability p (p is set to 0.2 or 0.5). A node may falsely accuse more than one neighboring node; however, it is only allowed to accuse a given node once. In order to increase the accuracy of the results, every simulation scenario runs 50 times with a simulation time of 600 seconds, and the average simulation results are calculated as the final data. The important simulation parameters are listed in Table 1.

5.2. Effectiveness of the Proposed Scheme

In this subsection, we evaluate the effectiveness of the proposed lightweight certificate revocation scheme in terms of revocation accuracy, and in particular, we examine the effectiveness of the wrong revocation recovery mechanism. To achieve this, the whole certificate revocation scheme described in this paper is named as ‘Our scheme’, and the scheme without the wrong revocation recovery mechanism is named as ‘Our scheme 1’. From 100 mobile nodes deployed in MANET, some are selected as malicious nodes. The number of malicious nodes is varied from 5 to 50 with an increment of 5 and the attack probability is set to 0.2 (or 0.5) for different simulation scenarios.

The accuracy of certificate revocation is defined as:

$$\text{Accuracy} = 1 - (R_{\text{wrong}} + R_{\text{unrevoked}}) / N_{\text{malicious}}, \quad (3)$$

Where R_{wrong} denotes the number of legitimate nodes which are wrongly revoked, $R_{\text{unrevoked}}$ is the number of malicious nodes which are not revoked and $N_{\text{malicious}}$ means the total number of malicious nodes deployed in the simulation runs.

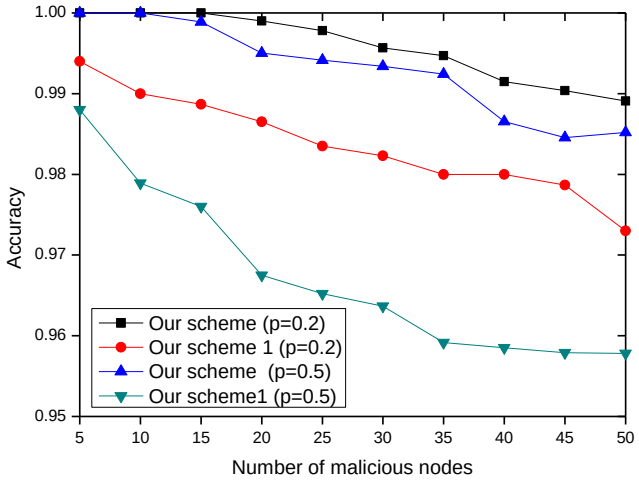

Figure 4. Revocation Accuracy

Figure 4 demonstrates the revocation accuracy of the two compared schemes. In the 'Our scheme 1', it works only with a certificate revocation strategy that if the accusation weight of the accuser is larger than that of the accused node, the certificate of the accused node is revoked. From the Figure 4 we can observe that this strategy can detect more than 97% of the malicious nodes when p is set to 0.2. Even though the attack probability is high to 0.5, this strategy still detects more than 95% of the malicious nodes. However, this strategy also can wrongly recognized legitimate nodes as malicious nodes and revoke their certificates. Consequently, the wrong revocation recovery mechanism is obviously important in the improvement of the accuracy of certificate revocation. Table 2 shows the number of nodes which have been wrongly revoked and finally recovered by wrong revocation recovery mechanism. This model works well in recognizing and recovering the falsely revoked nodes and results in clear improvement of the accuracy of certificate revocation as shown in Figure 4. We can notify that 'Our scheme' which equips with wrong revocation recovery mechanism achieves an obvious higher accuracy than 'Our scheme 1'. Consequently, we can conclude that the proposed lightweight certificate revocation scheme can effectively revoke the certificates of malicious nodes, especially with the help of the wrong revocation recovery mechanism.

Table 2. The Number of Recovered Wrongly Revoked Nodes

Number of malicious nodes	**5**	**10**	**15**	**20**	**25**	**30**	**35**	**40**	**45**	**50**
Number of recovered wrongly revoked nodes (p=0.2)	0.03	0.1	0.17	0.23	0.48	0.65	0.69	0.76	0.96	1.29
Number of recovered wrongly revoked nodes (p=0.5)	0.06	0.33	0.36	0.77	0.86	1.09	1.41	1.64	2.1	2.07

5.3. Comparing the Performance of Certificate Revocation Scheme

To verify that the proposed scheme inherits the merits of the voting-based scheme and

the non-voting-based scheme, the proposed scheme is compared with a voting-based scheme (RT is set to N/3) [15] and a non-voting-based scheme [20] in terms of revocation accuracy, revocation time and the number of accusations needed to revoke a certificate. The changes of the three metrics are examined in terms of different values of number of malicious nodes and node density.

In the first test scenario, we deploy 100 mobile nodes in the network, in which the number of malicious nodes are varied from 10 to 50 with an increment of 10 for each simulation. In the other scenario, the number of malicious nodes is fixed to 35 and the density of mobile nodes (including the malicious nodes) is varied from 60 to 100 nodes/km2 with an increment of 10 for each simulation. In all simulations, the attack probability (p) is set to 0.5.

Figure 5 andFigure **6** demonstrate the accuracy of certificate revocation impacted by the number of malicious nodes and the density of nodes, respectively. As expected from intuition, among the three schemes, the simulation results indicate that the voting-based scheme achieves a highest average accuracy when the number of malicious nodes is less than 30; the non-voting-based scheme works with a lowest average accuracy, and the accuracy of our proposed scheme is slightly lower than the voting-based scheme. In particular, as the number of malicious nodes is below N/3, the accuracy of voting-based scheme can reach 100 percent, however, when above the scheme's threshold (N/3), the accuracy drops dramatically. In contrast, our proposed scheme works smoothly with an accuracy of large than 98 percent, owing to the adoption of wrong revocation recovery mechanism. The increase of malicious nodes degrades the accuracy of certificate revocation because there are more malicious nodes take part in falsely accusing a legitimate node. On the other hand, higher node density improves the accuracy, as shown in Figure 6.

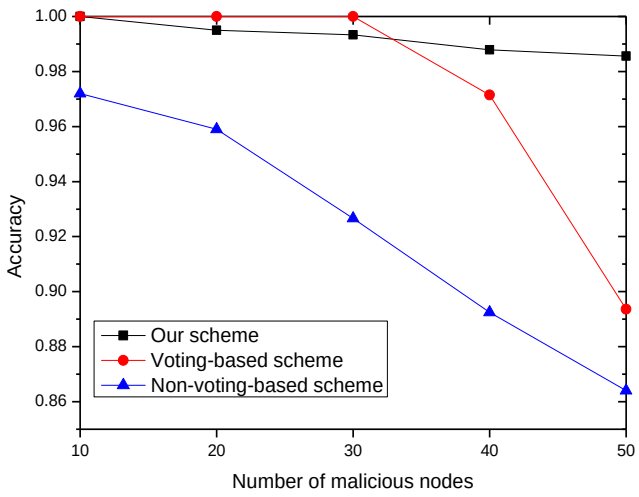

Figure 5. Impact of Malicious Nodes on Accuracy

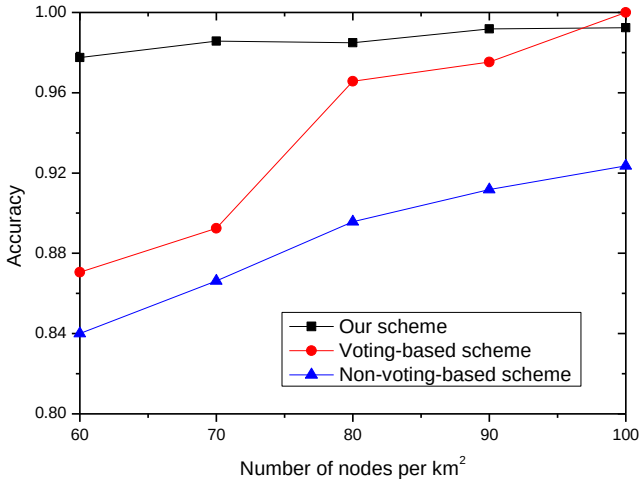

Figure 6. Impact of Node Density on Accuracy

Figure 7 and Figure **8** show us the average number of accusations required to revoke the certificate of a node. In this paper, other than the real accusation packets, the vindication packets are also deemed as accusation packet when calculating the average packet overhead for revocation schemes. As expected from intuition, the voting-based scheme needs obviously more accusations to revoke a certificate, because more nodes take part in the voting process. From the simulation results, we can observe that our scheme only need about 4 accusations to revoke the certificate of a node, which is slightly higher than that of the non-voting-based scheme (about 2 accusations). Among the 4 accusations needed in our proposed scheme, most of them are contributed by the real accusations. This can also explain the observation that the average accusations are not obviously influenced by the number of malicious nodes or the density of nodes. In contrast, in the non-voting-based scheme, one accusation is enough to revoke certificate, and the rest of the accusations are contributed by the vindication packets.

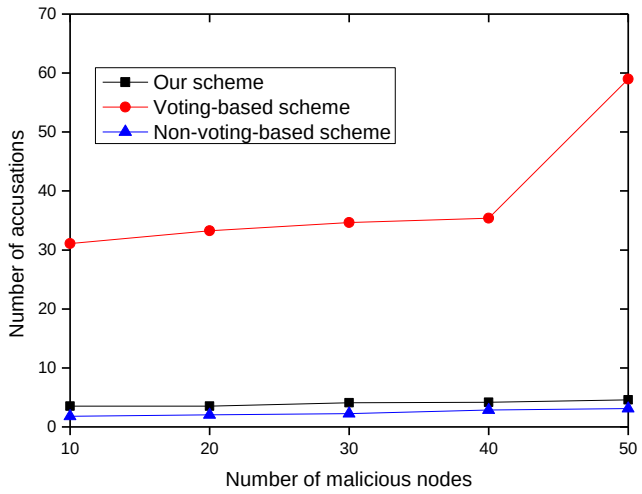

Figure 7. Impact of Malicious Nodes on Number of Accusations

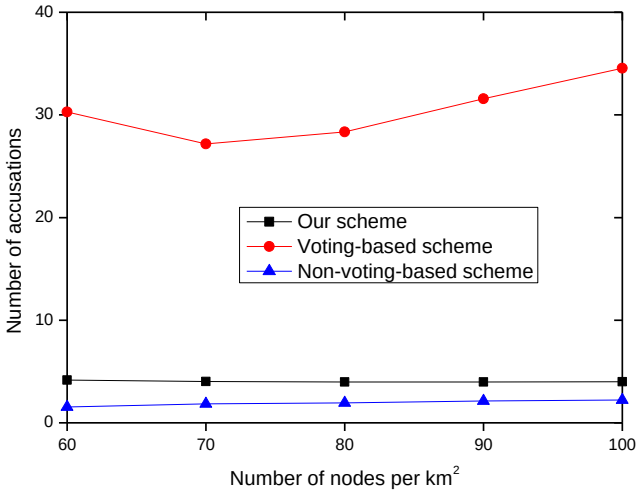

Figure 8. Impact of Node Density on Number of Accusations

Figure 9 and Figure **10** give another important metric for evaluating the performance of the revocation scheme - revocation time. Revocation time is defined as the time from a node first works maliciously until its certificate is revoked. We can observe that, the voting-based scheme consumes obviously longer revocation time than that of both our proposed scheme and the non-voting-based scheme, due to that the voting-based scheme always needs to wait for multiple votes to meet the conditions of certificate revocation. In contrast, the non-voting-based scheme requires only one single vote, and our proposed scheme needs small votes to make a decision. In addition, for this two schemes, the decrease of the node density or the increase of the number of malicious nodes results in the slightly increase of revocation time. Whatever conditions, the voting-based scheme has to take a long time to revoke the certificates of malicious node especially when the ratio of the malicious node increases.

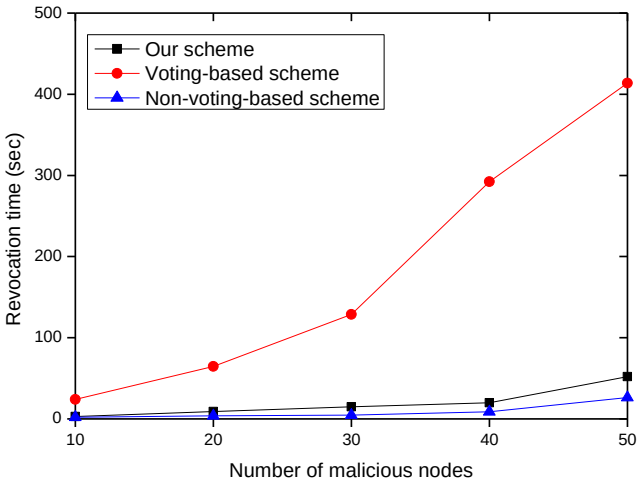

Figure 9. Impact of Malicious Nodes on Revocation Time

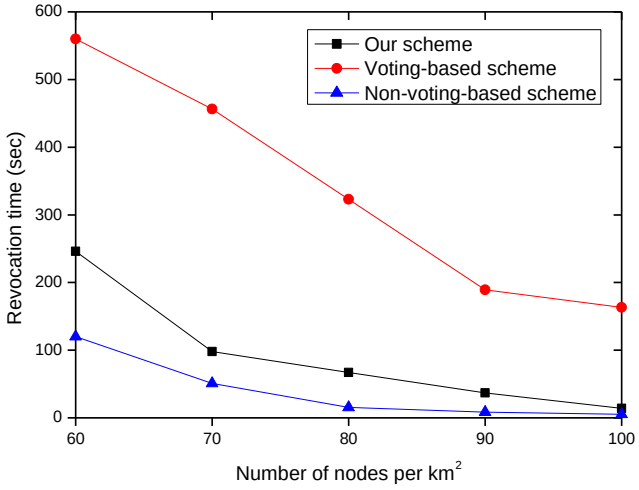

Figure 10. Impact of Node Density on Revocation Time

Consequently, we can summarize the simulation that, our proposed scheme can significantly reduce the revocation time and accusation overhead with a slight decrease of revocation accuracy, as compared with voting-based certificate revocation scheme. Particularly, our proposed scheme can also work effectively even if a larger number of malicious nodes exist in the network. Moreover, as compared with non-voting-based scheme, our scheme can achieve higher revocation accuracy with only a slight increase of revocation time and accusation overhead.

6. Conclusion

In this paper, we presented a lightweight certificate revocation scheme for hybrid mobile ad hoc networks. Our scheme is designed to retain the advantages of both voting-based and non-voting-based certificate revocation schemes. In order to ensure revocation accuracy, the scheme revoke the certificate of nodes based on weight-based multi-voting; meanwhile, to reduce the revocation time and overhead, the accused node is revoked immediately when its weight is less than the accuser. Thus, the accusations made by a few nodes can quickly revoke an accused node. Furthermore, to improve the accuracy, we have adopted a wrong revocation recovery mechanism to detect and recover the wrongly revoked nodes. In doing so, we have sufficient legitimate nodes to ensure the proposed scheme work effectively even in an environment with a high proportion of malicious nodes.

We have evaluated the performance of our scheme in a comparison way. The simulation results have demonstrated that our scheme achieves a performance trade-off: it obtains obvious higher revocation accuracy than non-voting-based scheme, and can revoke the certificate of a malicious node with notable shorter revocation time and fewer accusations compared with voting-based scheme.

Acknowledgments

This research is sponsored by the Natural Science Foundation of China (NSFC) under Grant No. 61202015 and 61401259, Research Fund for the Doctoral Program of Higher Education of China (RFDP) under Grant No. 20120131120033.

References

[1] R. Attia, R. Rizk, and H. A. Ali, "Internet connectivity for mobile ad hoc network: a survey based study", Wireless Networks, vol. 21, no. 7, **(2015)**, pp. 2369-2394.
[2] H. Xu, X. Cai, L. Ju, and Z. Jia, "Gateway pheromone–based adaptive internet access scheme for mobile ad hoc networks", International Journal of Ad Hoc and Ubiquitous Computing, vol. 19, no. 1-2, **(2015)**, pp. 50-61.
[3] H. 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, **(2004)**, pp. 38 - 47.
[4] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A Survey Of Routing Attacks In Mobile Ad Hoc Networks", IEEE Wireless Communications vol. 14, no. 5, **(2007)**, pp. 85 - 91.
[5] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks", IEEE Transactions on Vehicular Technology vol. 58, no. 5, **(2009)**, pp. 2471 - 2481.
[6] A. Prathapani, L. Santhanam, and D. P. Agrawal, "Detection of blackhole attack in a Wireless Mesh Network using intelligent honeypot agents", Journal of Supercomputing, vol. 64, no. 3, (2013), pp. 777-804.
[7] A. Nadeem, and M. Howarth, "Protection of MANETs from a range of attacks using an intrusion detection and prevention system", Telecommunication Systems, vol. 52, no. 4, **(2013)**, pp. 2047-2058.
[8] N. Shankar, and D. Balfanz, "Enabling secure ad-hoc communication using context-aware security services", Proceedings of UBICOMP2002 - Workshop on Security in Ubiquitous Computing, Göteborg,Sweden, **(2002)** September 29-October 1.
[9] R. Cabaniss, V. Kumar, and S. Madria, "Multi-party encryption (MPE): secure communications in delay tolerant networks", Wireless Networks, vol. 21, no. 4, **(2014)**, pp. 1243-1258.
[10] L. X. Qi Yue, Wan Yadong, "Low-Cost Round Encryption Method for Embedded System", International Journal of Security and its Applications, vol. 9, no. 4, **(2015)**, pp. 117-124.
[11] M. Almulla, Q. Zhang, A. Boukerche, and Y. Ren, "An efficient k-Means authentication scheme for digital certificates revocation validation in vehicular ad hoc networks", Wireless Communications & Mobile Computing, vol. 14, no. 16, **(2014)**, pp. 1546-1563.
[12] H. Yang, "SCAN: self-organized network-layer security in mobile ad hoc networks", IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, **(2006)**, pp. 261 - 273.
[13] K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks", IEEE 71st Vehicular Technology Conference (VTC 2010), Ottawa, Canada, **(2010)** September 6-9.
[14] M. A. Azer, S. M. El-Kassas, and M. S. El-Soudani, "Certification and Revocation Schemes in Ad Hoc Networks Survey and Challenges", Second International Conference on Systems and Networks Communications (ICSNC 2007), Cap Esterel, French Riviera, France, **(2007)** August 25-31.
[15] G. Arboit, C. Cre07Peau, C. R. Davis, and M. Maheswaran, "A localized certificate revocation scheme for mobile ad hoc networks", Ad Hoc Networks, vol. 6, no. 1, **(2008)**, pp. 17-31.
[16] C. Crépeau, and C. Davis, "A certificate revocation scheme for wireless ad hoc networks", Proceedings of Acm Workshop on Security of Ad Hoc and Sensor Networks, Fairfax,Virginia,USA, **(2003)**.
[17] N. Chaib, N. Lagraa, M. Yagoubi, and A. Lakas, "Unthresholded adaptive revocation technique in mobile ad hoc networks", Proceedings of Acm Symposium on Qos and Security for Wireless and Mobile Networks, Paphos,Cyprus, **(2012)** October 21-25.
[18] J. Clulow, and T. Moore, "Suicide for the common good: a new strategy for credential revocation in self-organizing systems", Sigops Oper.syst.rev, vol. 40, **(2006)**, pp. 18-21.
[19] W. Liu, H. Nishiyama, N. Ansari, and N. Kato, "A Study on Certificate Revocation in Mobile Ad Hoc Networks", 2011 IEEE International Conference on Communications (ICC2011), Kyoto,Japan, **(2011)** June 5-9.
[20] W. Liu, H. Nishiyama, N. Ansari, J. Yang, and N. Kato, "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks", IEEE Transactions on Parallel & Distributed Systems, vol. 24, no. 2, **(2013)**, pp. 239-249.
[21] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: Ubiquitous and Roubust Access Control for Mobile Ad Hoc Networks", IEEE/ACM Transactions on Networking, vol. 12, no. 6, **(2004)**, pp. 1049 - 1063.
[22] A. Hamidian, U. K02rner, and A. Nilsson, "Performance of Internet Access Solutions in Mobile Ad Hoc Networks", Proceedings of the First international conference on Wireless Systems and Mobility in Next Generation Internet, Dagstuhl Castle, Germany, **(2004)** June 7-9.

[23] D. Saravanan, R. M. Chandrasekaran, B. V. Prabha, and V. R. S. Dhulipala, "Trust Worthy Architecture Implementation for Mobile Ad hoc Networks", International Journal on Computer Science & Engineering, vol. 3, no. 7, **(2011)**, pp. 2601-2609.
[24] C. E. Perkins, "Royer :Ad-hoc on-demand distance vector routing", Proc.of IEEE Wksp.mobile Comp.sys. & Apps, vol. 6, no. 7, **(1999)**, pp. 90.

Authors

Huaqiang Xu, He is a lecturer, working in Shandong Normal university. Now he is pursuing the Ph.D. degree of Shandong University. His main research interests include wireless network routing protocol, embedded system and trust computing.

Rui Wang, He received the M.E. degree in the School of Software Engineering at Shandong University, in 2009. Now he is pursuing the Ph.D. degree of Shandong University. His main research interests include embedded systems, trust computing, Software Defined Networks and Software Defined Wireless Networks.

Zhiping Jia, He is a Professor and PhD supervisor of School of Computer Science and Technology, Shandong University. His main research interests include embedded system, trust computing, real-time scheduling, hardware/software Co-Designs, parallel and distributed systems.

