ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (326-333), Month: October - December 2014, Available at: www.researchpublish.com

Falsely Accused Node Discover Using End To End Scrutinize Method in Ad Hoc Networking

[1]S.Sivaraja, [2]N.Hemalatha

[1]Assistant Professor, Department of Computer Science, Kongu Arts and Science College, Erode, Tamil Nadu, India
[2]Research Scholar, Department of Computer Science (P.G), Kongu Arts and Science College, Erode, Tamil Nadu, India

***Abstract*: The certificate revocation is an important component to secure communication between wireless ad hoc networks. 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 this paper, Introduce two types of Windows Protocol namely specific window protocol and straightforward window protocol of which the latter produces the best output with slight increased calculation overheard.

In monitoring-based intrusion detection, each node monitors the forwarding behavior of its neighboring nodes in mobile ad hoc networks and produces the actual false positives result nearly similar to the real time environment. To identify the distributed attack and insider attack.. A new incentive method to release and restore the legitimate nodes and to improve the number of available normal nodes in the network has been proposed.

***Keywords*: Certificate Revocation, False Accusation, Ad hoc network, Intrusion Detection, MANET, Security.**

I. INTRODUCTION

A wireless mobile ad hoc network is a self-created, self organized and self-administering set of nodes connected via wireless links without the aid of any fixed infrastructure or administrator.

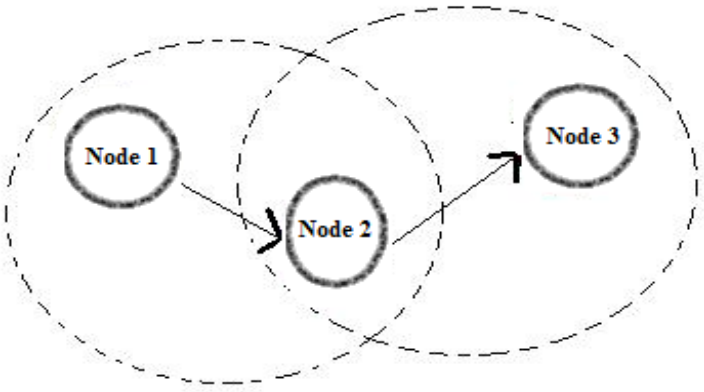


Fig. 1 Example of Mobile Ad-Hoc Network

Figure 1 shows a simple ad-hoc network with 3 nodes. Node 1 and node 3 are not within range of each other , however the node 2 can be used to forward packets between node1and node 2. The node 2 will act as a router and these three nodes together form an ad-hoc network

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (326-333), Month: October - December 2014, Available at: www.researchpublish.com

These attacks can be finding into following main objective types used:

- To verify that a public key belongs to an individual and to prevent tampering and forging
- To provide secure communications
- To mitigate malicious attacks on the network.
- To identified the attack as soon as possible.

II. EXISTING SYSTEM

Grouping or clustering is a process that divides the network into interconnected substructure known as groups. Each cluster having the cluster head (CH), cluster members.

The certificate revocation is an important component to secure communication between wireless ad hoc networks.

The certificate revocation process is quick and accurate for new novel Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme.

To improve the reliability of the scheme, to recover the warned nodes to take part in the certificate revocation process, to enhance the accuracy, to propose the threshold-based mechanism to assess and vindicate warned nodes as legitimate nodes or not, before recovering them.

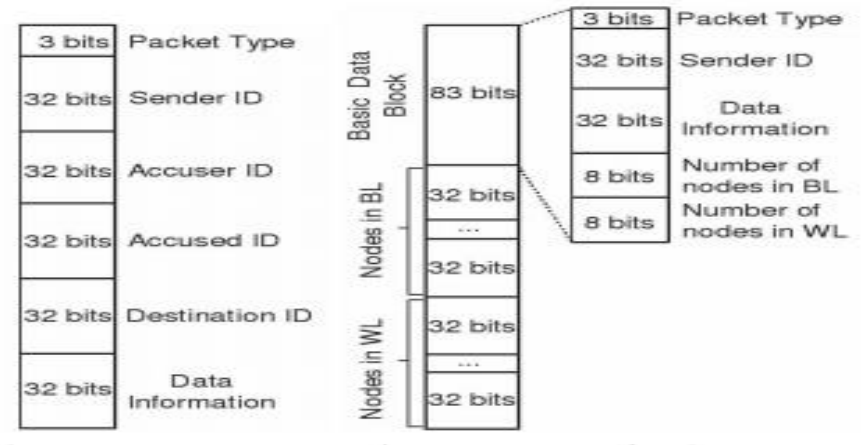
CA providing valid certificate to node present in the cluster as well as newly joining node in the cluster. In particular, to improve the reliability of the scheme wireless ad hoc network is divided into number of classification nodes and its (malicious node, attacker node and legitimate node) maintained as warning list (informer node) and black list (accused node) using voting and non-voting base detection mechanisms. Voting based mechanism is the process of revoking a malicious attacker's certificate through votes from valid neighboring nodes. Non-Voting based mechanism is the process of revoking the certificate of the node in the cluster network by any one of the node with valid certificate.

2.1 Function of Certificate Authority

A trusted third party, certification authority, is deployed in the cluster-based scheme to enable each mobile node to preload the certificate. The CA is also in charge of updating two lists, WL and Blacklist, which are used to hold the accusing and accused node information, respectively. The CA updates each list according to received control packets

2.2 Certificate Revocation

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



a) Format of accusation an Recover packets b) Format of broadcast packet.

Fig. 2 Control Packets

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (326-333), Month: October - December 2014, Available at: www.researchpublish.com

When a neighbor node indicates a particular node as a malicious node, Certificate Authority sends Accusation packet to the particular malicious nodes to conform before place in Black List. The informer node is placed in Warning List.

2.3 copying With False Accusation

The false accusation of a malicious node against a legitimate node to the CA, will degrade the accuracy and robustness of our scheme. After monitoring it sends recovery packet CA accepts the recovery packet and verifies the validity of the sender, the falsely accused node will be released from the BL and held in the WL. Furthermore, the CA propagates this information to all the nodes through the network. Fig.3 illustrates the process of addressing false accusation as follows:

Step 1: The CA disseminates the information of the WL and BL to all nodes in the network.

Step 2: CA updates its WL and BL, and determine that node B was framed.

Step 3: E and F send a recovery packet to the CA to revive the falsely accused node B.

Step 4: Upon receiving the first recovery packet (e.g., from E), the CA removes B from the BL and holds B and E in the WL and then disseminates the information to all the nodes.

Step 5: The nodes update their WL and BL to recover node B

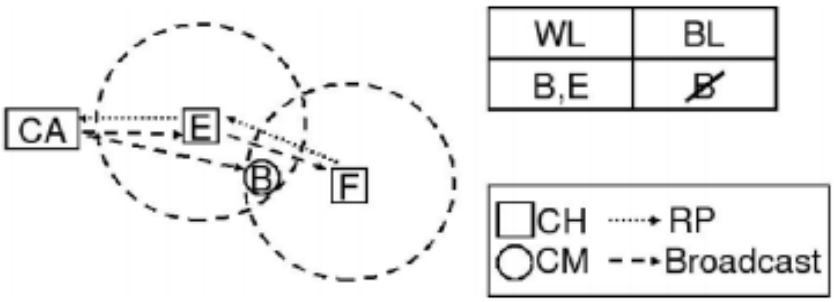


Fig. 3 Dealing with false accusation

Drawbacks of Existing System

- Vulnerable to various types of security attacks.
- Guarantee is challenge in secure network services.
- Identifying of any malicious attack is not possible.
- The false positive problem cannot be observed by simulating the same network using popular ad hoc network simulators.
- Exact quantitative evaluations of false positives in monitoring-based intrusion detection for ad hoc networks.
- Previous studies showed that the simulated network exhibits the aggregate false positive behavior but not much similar to real time high false positives.
- In Wireless networks that provide resilience to byzantine failures caused by individual or colluding nodes.
- Do not find the false accusation node details with in frequency communication.

III. PROPOSED SYSTEM

Two types of Windows Protocol namely specific window protocol and straightforward window protocol. In monitoring-based intrusion detection, each node monitors the forwarding behavior of its neighboring nodes. To identify the distributed attack and insider attack.

In most cases, a node only monitors its next hop in a route. For which a three-node segment of a route is considered (with at least two hops) being used to send data packets.. It produces the actual false positives result. Marko chain model is used

to find attackers and to identify the cluster member are within the communication frequency. Markov models are commonly used to analyze the expected time to encounter a bug in a software system.

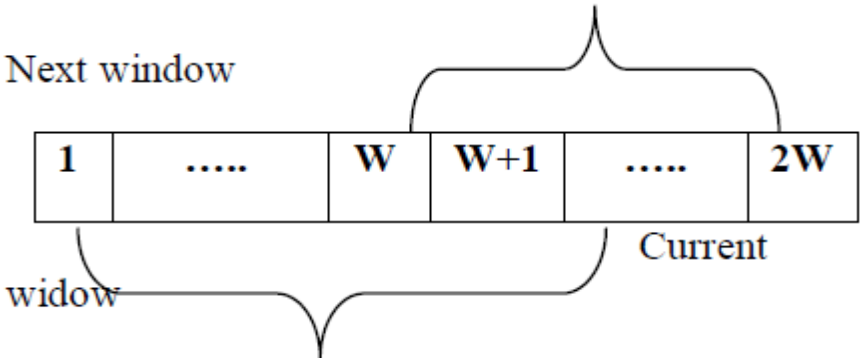
Straight forward window refers to imaginary boxes at the transmitter and receiver. straight forward window protocol assumes full duplex communication. It uses two types of frames, first data and second acknowledgment.

To understand the similarities and differences between the Specific and Straight forward windows, assume that noise does not impact the overhearing of transmission within a node's radio range. In such a scenario, a malicious node can drop up to L-1 packets out of W on the average without risking suspicion by neighbors. The temporary drop rates can be different.

The Straight forward window approach is free of this deficiency since in any consecutive W-transmitted packets, a malicious node may drop at most L-1 packets without risking suspicion by neighbors. To model the state of Straight forward window –based monitoring using a discrete-time Markov chain.

3.1 Specific Window Protocol

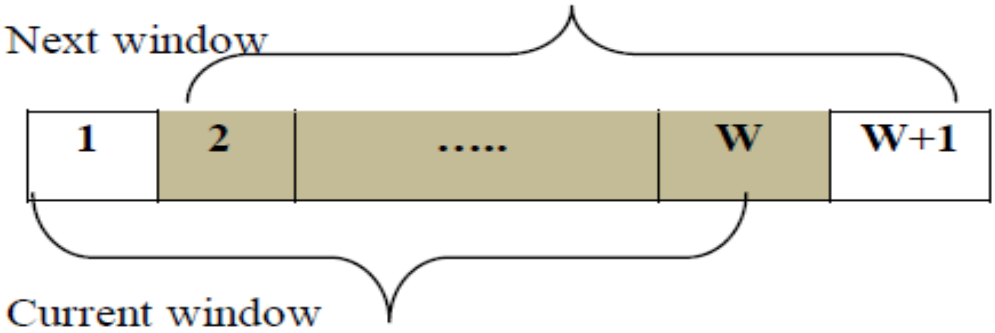
The Specific window protocol monitors the packet drops detection by checking the front and rear side of the packet. So the drop detection can be finding effectively.



Specific window

3.2 Straight Forward Window Protocol

The Straight forward window protocol monitors the packet drop detection in the sequence of packets. It is possible to reduce the number of false positive due to monitoring by having higher threshold values, allowing a node to exceed the not-overheard threshold multiple times before labeled as suspicious, or both. This mitigate the false positive problem in normal networks without attacks.



Straight forward window

The specific window protocol for sender node and receiver node transfer the data between ad-hoc networks through monitoring dropped packed and malicious node. In the straight window protocol for sender node and receiver node transfer the data between ad-hoc networks through monitoring sequences malicious node.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (326-333), Month: October - December 2014, Available at: www.researchpublish.com

IV. RESULTS AND DISCUSSION

Experimental Results

First design a simplified mechanism to determine the number of neighboring nodes for any given node. Within time *Tv*, the given node crosses through an area and meets a number of neighbors N. The mobile nodes are assumed uniformly distributed in the network, It may approximate N by

$$\mathbf{N} = (\pi r^2 + 2_{rv} T_v)\ \mathbf{p}$$

Where *r* denotes the transmission range of nodes, *v* is the velocity, and *p* is the density of nodes in the network. Based on the obtained number of neighboring nodes *N*, It can firm the value of threshold K.

Table 1 Existing System- Estimate malicious node

s.no	Revocation time (sec)	No.of attacker nodes	Average of attacker per mins (%)
1	100	125	3.68
2	200	195	10.67
3	300	356	25.38
4	400	384	38.22
5	500	475	60.41
6	600	566	90.63

The **Figure 4.1** represents experimental result for existing system. The finding malicious node and revocation node process within second details **Figure 4.2** shows Minutes details as followed.

The Table 1, 2 represents experimental result for proposed system. The finding malicious node and revocation node process within second, and Mines details as followed.

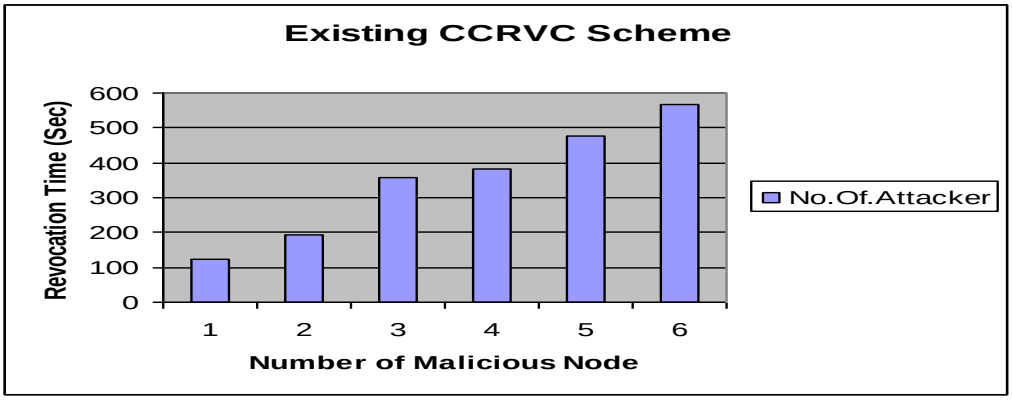


Figure 4.1 Existing System- Estimate malicious nodes

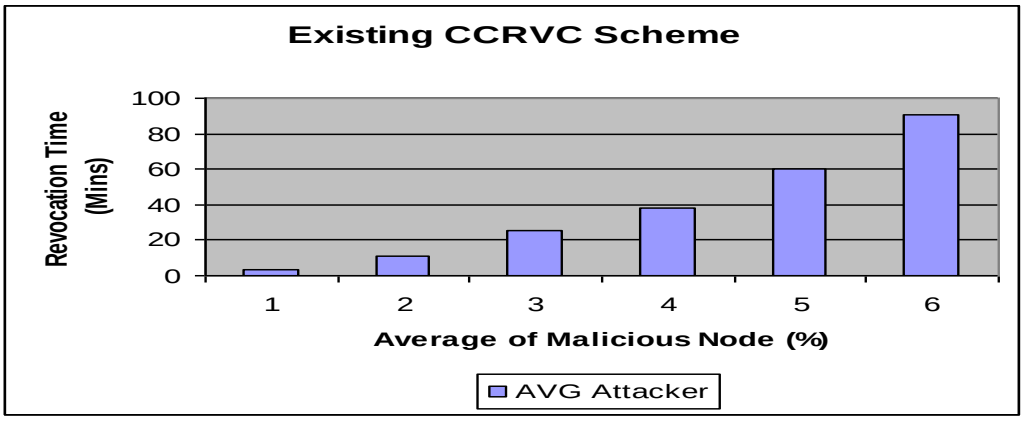


Figure 4.2 Existing System- Estimate malicious nodes (Min)

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (326-333), Month: October - December 2014, Available at: www.researchpublish.com

S. No	Falsely accused node discover	Existing ccrvc error rate (%)	Proposed ccrvc error rate (%)
1	100	2.89	2.84
2	200	3.42	3.16
3	300	4.33	4.04
4	400	5.28	5.13
5	500	6.05	5.96
6	600	6.98	6.82
7	700	7.32	7.26
8	800	8.15	8.06
9	900	9.02	8.89
10	1000	9.34	9.15

The Figure 4.3, fig 3 for existing system. The finding malicious node and revocation node process within second, min details as followed.

The Figure 4.4 for comparison of existing CCRVC and proposed CCRVC system. The finding falsely accused node discovery error rate within cluster communication details as followed.

Table 2 Proposed System- Estimate malicious node

S. No	Revocation time (sec)	No. of attacker nodes	Average of attacker per mins (%)
1	100	134	4.18
2	200	213	12.37
3	300	383	35.78
4	400	405	40.12
5	500	487	63.46
6	600	625	93.13

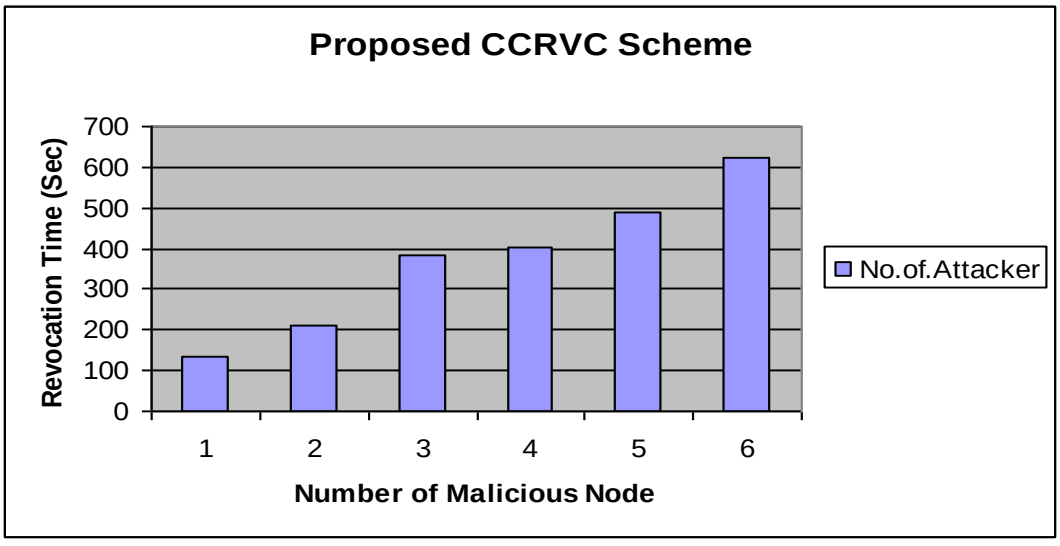


Figure 4.3 Proposed System- Estimate m alicious node

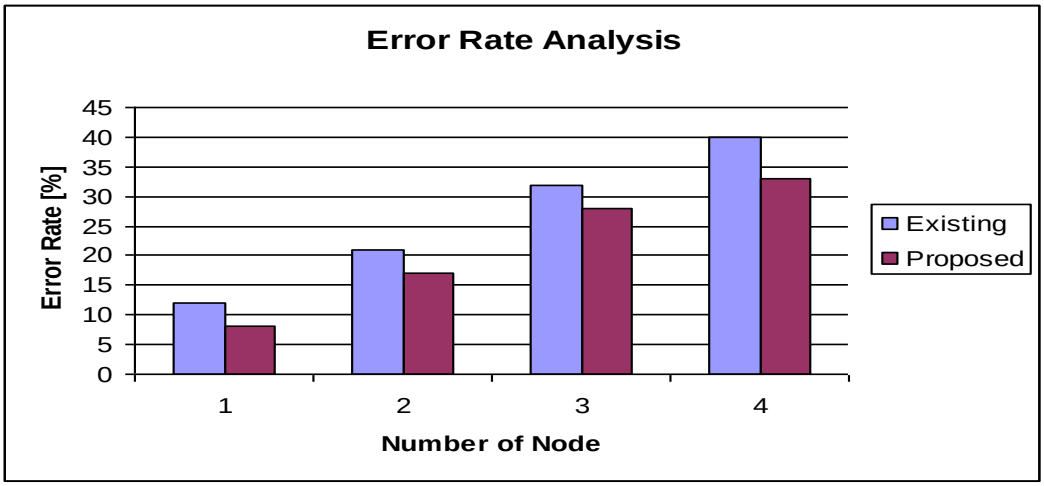


Figure 4.4 Comparison - Existing CCRVC and Proposed CCRVC System (Error Rate)

V. CONCLUSION

The proposed system eliminates the difficulties in the existing system. In this thesis, major issues to ensure secure communications for mobile ad hoc networks, namely, certificate revocation of attacker nodes are solved. In contrast to existing algorithms, propose a cluster-based certificate revocation with vindication capability scheme combined with the merits of both voting-based and non-voting based mechanisms to revoke malicious certificate and solve the problem of false accusation. A new incentive method to release and restore the legitimate nodes and to improve the number of available normal nodes in the network has been proposed. This software is very particular in finding malicious applications.

VI. FUTURE ENHANCEMENT

The process of preparing plans had been a new experience, which was found useful in later phases of the project is completed. Efforts had been taken to make the system user friendly and as simple as possible. However at some points some features may have been missed out which might be considered for further modification of the application. The new system become useful if the below enhancements are made in future.

- Attack finding and identified using new certificated scheme by NP Hard problem solve.
- Finding attacker using packet drop identifying AI application, Mitigate malicious attacks on the network.

REFERENCES

[1] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Comm., vol. 11, no. 1, pp. 38-47, Feb. 2004.

[2] P. Sakari ndr and N.Ansari , "Security Services in Group Communications Over Wireless Infrastructure, Mobile Ad Hoc, and Wireless Sensor Networks," IEEE Wireless Comm., vol. 14, no. 5, pp. 8-20, Oct. 2007.

[3] L. Zhou, B. Cchneider, and R. Van Renesse, "COCA: A Secure Distributed Online Certification Authority," ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.

[4] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Nov./Dec. 1999.

[5] L. Zhou, B. Cchneider, and R. Van Renesse, "COCA: A Secure Distributed Online Certification Authority," ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.

[6] C. Gentry, "Certificate-Based Encryption and the Certificate Revocation Problem," EUROC RYPT: Proc. 22nd Int 'l Conf. Theory and Applications of Cryptographic Techniques, pp. 272-293, 2003.

[7] H. Yang, J. Shu, X. Meng, and S. Lu, "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 261-273, Feb. 2006.

[8] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Network: Analysis & Defenses," Proc. Third Int'l Symp. Information Processing in Sensor Networks, pp. 259-268, 2004.

[9] W. Liu, H. Nishiyama, N. Ansari, and N. Kato, "A Study on Certificate Revocation in Mobile Ad Hoc Network," Proc. IEEE Int'l Conf. Comm. (ICC), June 2011.

[10] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, "Resisting Flooding Attacks in Ad Hoc Networks," Proc. Int'l Conf. Information Technology: Coding and Computing, 2005.

[11] Kong, X. Hong, Y. Yi, J.-S. Park, J. Liu, and M. Gerla, "A Secure Ad-Hoc Routing Approach Using Localized Self-Healing Com-munities," Proc. Sixth ACM Int'l Symp. Mobile Ad hoc Networking and Computing , pp. 254-265. 2005.

[12] V. Davies. Evaluating mobility models within an ad hoc network. Master's thesis, Colorado School of Mines, 2000.

[13] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad hoc Net work Research," Wireless Comm. and Mobile Computing (WCMC) Special Issue on Mobile Ad Hoc Networking: Research, Trends, and Applications, vol. 2, no. 5, pp. 483-502, 2002.

[14] M. Sanchez and P. Manzoni. Anejos: A java based simulator for ad-hoc networks. Future Generation Computer Systems, 17(5):573–583, 2001.

[15] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Nov./Dec. 1999.

[16] C. Gentry, "Certificate-Based Encryption and the Certificate Revocation Problem," EUROC RYPT: Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques, pp. 272-293, 2003.

[17] IEEE-SA Standards Board, "IEEE Std. 802.15.4," IEEE, 2003.

[18] Bing Wu, Jie Wu , Yuhong Dong, "An Efficient group key management scheme for mobile ad hoc networks",Int. J. Security and Networks, Vol.

[19] Lidong Zhou and Zygmunt J.Hass, "Securing Ad Hoc Networks", Cornell University,IEEE Network, November/December 1999.

[20] E. Ayanoglu, C . L. I, R. D. Gitlin, and J. E. Mazo. Diversity coding for transparent self-healing and fault-tolerant communication networks. IEEE Transactions on Communications , 41(11):1677–1686, Nove mb e r 1993.