ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

Packet Hiding Methods for MANET Routing Attacks

Mrs.K.Rajasri[1], R.Anudeeparani[2], R.Prema[3], R.Vasugi[4]

Senior Assistant Professor, CSE, Christ College of Engg & Tech, Pondicherry, India[1]

Student, CSE, Christ College of Engg & Tech, Pondicherry, India[2]

Student, CSE, Christ College of Engg & Tech, Pondicherry, India[3]

Student, CSE, Christ College of Engg & Tech, Pondicherry, India[4]

Abstract: Mobile ad hoc networks (MANETs) have been highly susceptible due to the flexibility provided by their dynamic infrastructure. The routing attacks could cause severe damage to MANET. Although there are several intrusion response techniques to alleviate such critical attacks, existing solutions normally attempt to isolate malicious nodes based on binary or naı¨ve fuzzy response decisions. Though, binary responses may effect in the unpredicted network partition, producing extra damages to the network communication. However, this flexibility introduces new security threats such as routing attacks, Denial-of-Service and selective jamming attacks. Many existing security solutions for conventional networks are ineffective and inefficient for many predicted MANET deployment environments. In our project, we address the problem of routing attacks, Denial-of-Service and selective jamming attacks in mobile ad hoc networks. Therefore, we propose that these MANET routing attacks can be introduced by the real-time packet classification. In such attacks, the rival remains active only for a short span, selectively aiming at highly significant messages. We exemplify the benefits of selective jamming in terms of rival effort and network performance degradation with a selective jamming attack on TCP and another on routing. We explain that selective jamming attacks can be introduced by the real-time packet classification. To alleviate these attacks, we build up schemes that evade real-time packet classification by merging cryptographic primitives. We evaluate the security of our techniques and compute their computational and communication overhead.

Keywords: MANET (Mobile Ad-hoc Networks), Selective Jamming, Denial-of-Service, Wireless Networks, Packet Classification.

I. INTRODUCTION

Mobile computing is a technology that lets to transmit data by means of a computer, without connecting to a fixed physical link. An expansion of this technology has the capacity to forward and accept data across these mobile networks. The data communication in the mobile networks has become vital and quickly developing technology since it let users to send data from remote locations to other remote or fixed locations. This illustrates the key to the biggest crisis of business people on the move that is, mobility.

A. Mobile Ad-hoc Networks

Mobile Ad-hoc Network can be organized as an infrastructure less network which are connected to mobile devices. Every device in a MANET can move independently in any direction, and so it can change its link to other devices frequently. Every device must send traffic irrelevant to its own reason, and Hence it may be router. The major dispute in constructing a MANET is to offer every device to maintain the information continuously which is required to appropriately route traffic. Such kind of networks can function by themselves or it can be linked to the internet.

MANETs are one of the kinds of wireless ad-hoc networks which can vary positions and organize itself on the fly. Since MANETs are mobile, they utilize wireless links to connect to different networks. Mobile Ad-hoc network (MANET) is a set of autonomous mobile nodes which can communicate every other by means of radio waves. The mobile nodes that are within radio range of every other can directly communicate, whereas other needs the aid of middle nodes to way their packets. These networks are completely spread, and can labor at some area devoid of the aid of any infrastructure. This characteristic makes these networks highly flexible and robust.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

Fig.1.1 Mobile Ad-hoc Network

B. Characteristics of MANET

- Communication by means of wireless channels.
- Nodes can function as both hosts and routes.
- No centralized controller and infrastructure.
- Active network topology.
- Recurrent routing updates.
- Independent, no infrastructure needed.
- Can be set at any location.
- Energy restraints.
- Inadequate security.

Congestion in point-to-point transmissions in a wireless mesh network may have devastating effects on data transfer via the network. The effects of jamming at the physical layer reverberate through the protocol stack, providing an effective denial-of-service (DoS) attack on end-to-end data communication. Yet, current work has established that perceptive jammers can include intersect layer protocol data into jamming attacks, lowering source spending by various orders of magnitude by aiming certain link layer and MAC performance healthy as link layer error detection and correction protocols. Hence, more experienced anti-jamming methods and protective scopes must be included into higher-layer protocols, for example channel surfing or routing relatively jammed sectors of the network.

The most of anti- jamming methods make use of multiplicity. For example, anti- jamming protocols may utilize different frequency bands, different MAC channels, or different routing paths. Such multiplicity methods help to check the effects of the jamming attack by demanding the jammer to act on different benefits together. In this project, we deal with the anti-jamming variety based on the use of different routing paths. Using different-path modification of source routing protocols such as Active Source Routing (DSR) or Ad-Hoc On-Demand Distance Vector (AODV), for example the MP-DSR protocol, every source node can demand various routing paths to the goal node for simultaneous use. To make productive use of this routing multiplicity, yet, every source node must be able to make an intelligent part of traffic beyond the accessible paths while permitting for the potential effect of jamming on the resulting data throughput.

In order to differentiate the effect of jamming on throughput, every source must get together the data on the crash of the jamming attack in different parts of the network. Yet, the amount of jamming at every network node requires on a number of nameless parameters, counting the approach used by the exacting jammers and the qualified spot of the jammers with respect to every transmitter-receiver pair. Hence, the crash of jamming is probabilistic from the viewpoint of the network1, and the classification of the jamming forces extra complex by the actuality that the jammers' strategies may be active and the jammers themselves may be mobile.

Thus we examine the capability of network nodes to describe the jamming effect and the capability of different source nodes to offset for jamming in the assign on of traffic across different routing paths.

Our supports to this problem are as follow:

1. We plan the problem of assigning traffic across different routing paths in the occurrence of jamming as a lossy network arise optimization problem. We plot the optimization problem to that of benefit part using portfolio selection theory.

2. We originate the federalized traffic allotment problem for different source nodes as a curved optimization problem.

3. We illustrate that the multi-source different-path optimal traffic allotment can be formulated at the source nodes using a dispersed algorithm based on decay in network service maximization.

4. We suggest methods which permit particular network nodes to nearby describe the jamming effect and collective this information for the source nodes.

Routing has been a dynamic part in wireless networking study. Most of the unique work in this spot embattled high-mobility scenarios such as arena networks. Hence, the center was on beginning and retaining routes in normal and random changes in network connectivity. A number of on-demand routing protocols have been future for this reason, as represented by DSR and AODV, where packets are routed along paths with the smallest bound calculate. Newly, wireless mobile ad hoc networks have

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

appeared as a new major application of multi hop wireless networks. Nodes in such networks have small or no mobility and frequently are not forced by little battery-life or partial computational power. Hence, civilizing network actions develop into the main center. Studiers have establish that the hop-count metric, as used in DSR and AODV, does not offer good action since not all hops are equivalent. To adopt this matter, different link-value metrics have been suggested. We express that the use of set selection theory permits the data sources to stability the predictable data throughput with the indecision in feasible traffic rates.

II. EXISTING SYSTEM

Jamming attacks are difficult to counter and more security problems may arise. They have been illustrated to actualize severe Denial-of-Service (DoS) attacks beside wireless networks. In the simplest way of jamming, the opponent interferes with the response of messages by transmitting a constant jamming signal, or several little jamming pulses jamming attacks have been considered in an external threat model, in which the jammer is not branch of the network. In this model, jamming strategies embrace the constant or random transmission of high- power meddling signals. The jammer was located within the proximity of one of the intermediate hops of the TCP connection. The intentional meddling with wireless communications can be employ as a arise pad for mounting Denial-of-Service attacks on wireless networks. In these attacks, the rival is active only for a short span, selectively aiming at highly significant messages.

A. *Extended Dempster- Shafer Theory of Evidence*

There is an extended d-s evidence model with importance factors and articulate expected properties for dempster's rule of combination with importance factors (DRCIF). D-S theory has been adopted as a valuable tool for evaluating reliability and security in information systems and by other engineering fields, where precise measurement is impossible to obtain or expert elicitation is required. D-S theory has several characteristics. First, it enables us to represent both subjective and objective evidences with basic probability assignment and belief function. Second, it supports Dempster's rule of combination (DRC) to combine several evidences together with probable reasoning. However, Dempster's rule of combination has several limitations, such as treating evidences equally without differentiating each evidences and considering priorities among them. To address these limitations in MANET intrusion response scenario, we make use of a new Dempster's rule of combination with a notion of importance factors (IF) in D-S evidence model. The risk-aware approach is based on the extended D-S evidence model. Dempster's rule of combination with importance factors is non associative and weighted, which has not been addressed in the literature. We propose an adaptive risk-aware response mechanism with the extended d-s evidence model, considering damages caused by both attacks and countermeasures. The adaptiveness of our mechanism allows us to systematically cope with MANET routing attacks.

Importance factor (IF) is a positive real number associated with the importance of evidence. IFs are derived from historical observations or expert experiences.

An evidence E is a 2-tuple (m,IF), where m describes the basic probability assignment. The basic probability assignment which describes the combined evidence,

$$m(C) = \frac{\sum_{A_i \cap B_j = C} m_1(A_i) m_2(B_j)}{1 - \sum_{A_i \cap B_j = \phi} m_1(A_i) m_2(B_j)}$$

The proposed rule of combination with importance factors should be a superset of Dempster's rule of combination. In this, we describe four expected properties that are Dempster's rule of combination with importance factors should follow. Properties 1 and 2 ensure that the combined result is valid evidence. Property 3 guarantees that the original Dempster's Rule of Combination is a special case of Dempster's Rule of Combination with importance factors, where the combined evidences have the same priority. Property 4 ensures that importance factors of the evidences are also independent from each other.

The risk-aware approach is based on the extended D-S evidence model.

B. *Risk Aware Mechanism*

1. Evidence collection

In this step, Intrusion Detection System (IDS) gives an attack alert with a confidence value, and then Routing Table Change Detector (RTCD) runs to figure out how many changes on routing table are caused by the attack.

2. Risk assessment

Alert confidence from IDS and the routing table changing information would be further considered as independent evidences for risk calculation and combined with the extended D-S theory. Risk of countermeasures is calculated as well during a risk assessment phase. Based on the risk of attacks and the risk of countermeasures, the entire risk of an attack could be figured out.

3. Decision making

The adaptive decision module provides a flexible response decision making mechanism,

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

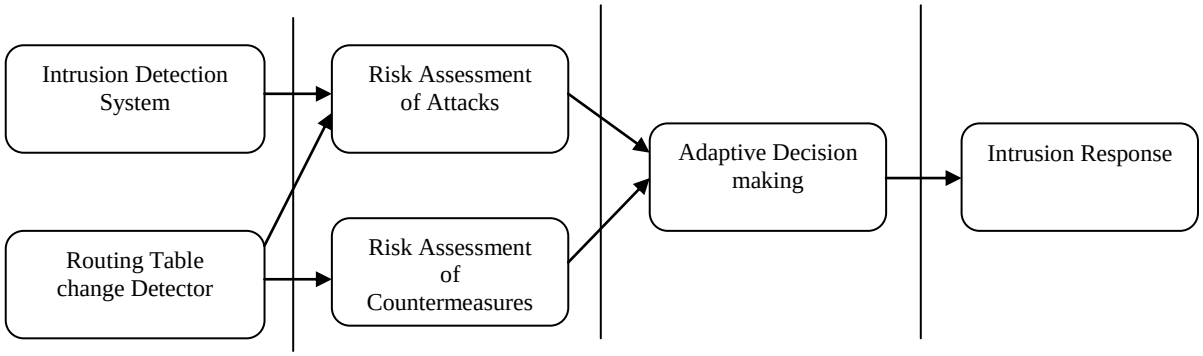

Fig 2.1: Risk-aware response mechanism

which takes risk estimation and risk tolerance into account. To adjust temporary isolation level, a user can set different thresholds to fulfill their goal.

4. Intrusion response

With the output from risk assessment and decision-making module, the corresponding response actions, including routing table recovery and node isolation, are carried out to mitigate attack damages in a distributed manner.

5. Routing table recovery

Routing table recovery is an indispensable response and should serve as the first response method after successful detection of attacks. In proactive routing protocols like OLSR, routing table recovery does not bring any additional overhead since it periodically goes with routing control messages. Also, as long as the detection of attack is positive, this response causes no negative impacts on existing routing operations.

C. *Disadvantages of Existing System:*

- Broadcast communications are particularly susceptible in an internal threat model because all deliberate receivers must be alert of the covert used to guard broadcast.
- The shared nature of the wireless channel permits it defenseless to intended interference attacks, typically referred to as jamming.
- Anyone with a transceiver can snoop on wireless communications, introduce false messages, or jam justifiable ones.
- Therefore, the negotiation of a single receiver is adequate to reveal relevant cryptographic information.

III. PROPOSED SYSTEM

An experienced adversary who is conscious about network secrets and the functioning of network protocols at a few layers in the network stack is considered. The adversaries utilize his internal knowledge for introducing selective jamming attacks in which particular messages of "high significance" are embattled.

A. *Response to Routing Attacks*

In our approach, we use two different responses to deal with different attack methods: routing table recovery and node isolation.

1. Routing table recovery

Routing table recovery includes local routing table recovery and global routing recovery. Local routing recovery is performed by victim nodes that detect the attack and automatically recover its own routing table.Global routing recovery involves with sending recovered routing messages by victim nodes and updating their routing table based on corrected routing information in real time by other nodes in MANET.

Routing table recovery is an indispensable response and should serve as the first response method after successful detection of attacks. In proactive routing protocols like OLSR, routing table recovery does not bring any additional overhead since it periodically goes with routing control messages. Also, as long as the detection of attack is positive, this response causes no negative impacts on existing routing operations.

2. Node isolation

Node isolation may be the most intuitive way to prevent further attacks from being launched by malicious nodes in MANET. To perform a node isolation response, the neighbors of the malicious node ignore the malicious node by neither forwarding packets through it nor accepting any packets from it. On the other hand, a binary node isolation response may result in negative impacts to the routing operations, even bringing more routing damages than the attack itself.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

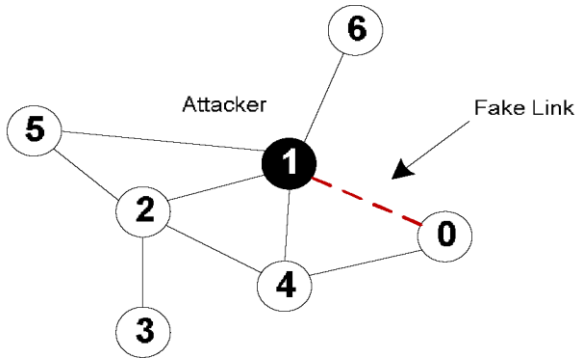

Fig 3.1: Example Scenario

For example, in Fig. 3.2, Node 1 behaves like a malicious node. However, if every other node simply isolate Node 1, Node 6 will be disconnected from the network. Therefore, more flexible and fine-grained node isolation mechanism are required.

In our risk-aware response mechanism, we adopt two types of time-wise isolation responses: temporary isolation and permanent isolation. The response action and band boundaries are all determined in accordance with risk tolerance and can be changed when risk tolerance threshold changes. The upper risk tolerance threshold (UT) would be associated with permanent isolation response. The lower risk tolerance threshold (LT) would remain each node intact. The band between the upper tolerance threshold and lower tolerance threshold is associated with the temporary isolation response, in which the isolation time (T) changes dynamically based on the different response level.

In these existing system we seen risk aware mechanism and d-s theory both considered after attacks and dos attacks to overcome we used before attacks to find, dos and jamming attacks before attacks we can find using cost sensitive naïvefuzzy response in these mechanism. We propose an adaptive risk-aware response mechanism with the extended D-S evidence model, considering damages caused by both attacks and countermeasures. The adaptiveness of our mechanism allows us to systematically cope with MANET routing attacks. We evaluate our response mechanism against representative attack scenarios and experiments. Our results clearly demonstrate the effectiveness and scalability of our risk-aware approach.

For instance, a jammer can target route-request/route-reply messages at the routing layer to inhibit route discovery, or end TCP acknowledgments in a TCP assembly to strictly break down the throughput of an end-to-end flow. In order to introduce selective jamming attacks, the adversary must be able to implement a "classify-then-jam" strategy before the end of a wireless transmission. Such method can be done moreover by classifying transmitted packets with protocol semantics, or by cracking packets on the wing.

In these decoding packets on the fly method, the jammer may decode the first little bits of a packet for civilizing valuable packet classifiers such as packet kind, source and destination address. Behind categorization, the opponent must bring on a adequate number of bit errors so that the packet can't be improved at the receiver. Selective jamming requires informal information of the physical (PHY) layer, on top of the facts of upper layers.

To mitigate the attacks, we develop a scheme that prevents real-time packet classification by combining cryptographic primitives with physical-layer attributes. We illustrated that the jammer can categorize communicated packets in real time by translating the first little symbols of an ongoing transmission, but by using OLSR algorithm using naïve fuzzy logic the jammer cannot decode the first few symbols of the transmitted packet. We examine the security levels of our methods and we illustrate that the problem of real-time packet classification can be plotted to the hiding property of commitment schemes, and intend a packet-hiding scheme based on commitments.

B. *Advantages Of Proposed System:*

✓ Relatively simple to actualize by developing information of network protocols and cryptographic primitives take out from negotiated nodes.

✓ Our resultings point out that selective jamming attacks guide to DoS with very low strength on behalf of the jammer.

✓ Achieve strong security properties.

C. *Proposed System Algorithm*

We suggest a solution based on Optimized Link State Routing (OLSR) protocol that initiates an unassuming transmission and calculation overhead. Such alterations were initially suggested by Rivest to reduce brute force attacks beside block encryption algorithms. An optimized link state routing (OLSR) protocol serves as a publicly known and completely invertible pre-processing step to a plaintext before it is agreed to a common block encryption algorithm.

In our context, packets are pre-processed by an optimized link state routing (OLSR) protocol before transmission but stay unencrypted. The jammer cannot execute packet classification until all pseudo-messages corresponding to the unique packet have been expected and the reverse transformation has been applied.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

D. *Algorithm Description*

The formal description of the Optimized Link State Routing for reducing routing overhead in route discovery is illustrated in the following Algorithm.

E. *Algorithm OLSR*

Definitions:

RREQv: RREQ packet received from node *v*.

Rv.id: the unique identifier (id) of *RREQv*.*N*(*u*): Neighbor set of node *u*.

Partition U(*u*, *x*): Uncovered neighbors set of node *u* for RREQ whose id is *x*.

Timer(*u*, *x*): Timer of node *u* for RREQ packet whose id is *x*.

*{*Note that, in the actual implementation of OLSR protocol, every different RREQ needs a UCN set and a Timer.*}*

1. if *ni* receives a new *RREQs* from *s* then

2. *{*Compute initial uncovered neighbors set*U*(*ni*,*Rs.id*) for *RREQs*:*}*

3. *U*(*ni*,*Rs.id*) = *N*(*ni*) - [*N*(*ni*) *n N*(*s*)] - *{s}*4: *{*Compute the *Dempster rule for delay Td*(*ni*):*}*

4. *Tp*(*ni*) = 1 -|*N*(*s*)*nN*(*ni*)| |*N*(*s*)|

5. *Td*(*ni*) = *MaxDelay* × *Tp*(*ni*)

6. Set a Timer(*ni*,*Rs.id*) according to *Td*(*ni*)

7. end if

8. while *ni* receives

a duplicate *RREQj* from*nj* before
9. Timer(*ni*,*Rs.id*) expires
do 11: *{*Adjust *U*(*ni*,*Rs.id*):*}*

10. *U*(*ni*,*Rs.id*)=*U*(*ni*,*Rs.id*)-[*U*(*ni*,*Rs.id*)*nN*(*nj*)]

11. discard(*RREQj*);

12. end while

13. if Timer(*ni*,*Rs.id*) expires then

14. *{*Compute the *Temporary Destination of PacketHiding Pre*(*ni*):*}*

15. *Ra*(*ni*) =|*U*(*ni*,*Rs.id*)| |*N*(*ni*)|

16. *Fc*(*ni*) = *Nc* |*N*(*ni*)|

17. *Pre*(*ni*) = *Fc*(*ni*) · *Ra*(*ni*) step to 19: if Random(0,1) = *Pre*(*ni*) then

18. Forward-Relay(*RREQs*)

19. else

20. discard(*RREQs*)

21. end if

22. end if

IV. CONCLUSION

The selective jamming attacks and Denial-of-Service attacks in wireless networks was addressed. An internal rival model in which the jammer is element of the network in attack, thus being alert of the protocol provisions and collective network furtive is considered. The jammer can categorize send out packets in concurrent by translating the first little symbols of an ongoing transmission was illustrated. The crash of selective jamming attacks on network protocols such as TCP and Routing was evaluated. The findings illustrate that a selective jammer can significantly crash performance with very low effort. There are three schemes that are developed to convert a selective jammer to a chance one by avoiding concurrent packet categorization. The schemes merge cryptographic primitives such as commitment schemes, cryptographic puzzles, and (OPTIMIZED LINK STATE ROUTING (OLSR)) with physical layer characteristics. The security of the schemes were analysed and quantified its computational and communication overhead. The jamming attack of inducing spurious messages into the data packets was addressed. It was prevented by using OPTIMIZED LINK STATE ROUTING (OLSR) method so that the jammer will not be able to view or put any spurious message unless all the bits have been obtained completely. This protects the data to reach the destination by the time the adversary tries to induce illegitimate messages. Jamming attacks on voice communications have been launched since the 1940s. In the context of digital communications, the jamming problem has been addressed in various threat models. We present a classification based on the selective nature of the adversary.

ACKNOWLEDGEMENT

The research leading to these results received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreements 215483(S-Cube) and 257483 (Indenica).

REFERENCES

[1] J. D. Abdulai, M. Ould-Khaoua, and L. M. Mackenzie, "Civilizing Probabilistic Route Discovery in Mobile Ad Hoc Networks," Proc. of IEEE Conference on Local Computer Networks, pp. 739-746, 2007.
[2] J. D. Abdulai, M. Ould-Khaoua, L. M. Mackenzie, and A. Mohammed, "Neighbour Coverage: A Active Probabilistic Route Discovery for Mobile Ad hoc Networks," *Proc. of SPECTS'08, pp. 165-172*, 2008.
[3] H. AlAamri, M. Abolhasan, and T. Wysocki, "On Optimising Route Discovery in Absence of Previous Route Information in MANETs," *Proc. of IEEE VTC 2009*-Spring, pp. 1-5, 2009.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

[4] J. Chen, Y. Z. Lee, H. Zhou, M. Gerla, and Y. Shu, "Robust Ad Hoc Routing for Lossy Wireless Environment," *Proc. of MILCOM'06, pp. 1-7*, 2006.
[5] Z. Haas, J. Y. Halpern, and L. Li, "Gossip-based Ad hoc Routing," *Proc. IEEE INFOCOM'02,* vol. 21, pp. 1707-1716, 2002.
[6] D. Johnson, Y. Hu, and D. Maltz, "The Active Source Routing Protocol for Mobile Ad hoc Networks (DSR) for IPv4," *RFC 4728*, 2007.
[7] A. Keshavarz-Haddady, V. Ribeirox, and R. Riedi, "DRB and DCCB: Efficient and Robust Active Broadcast for Ad Hoc and Sensor Networks," Proc. of SECON'07, pp. 253-262, 2007.
[8] J. Kim, Q, Zhang, and D. P. Agrawal, "Probabilistic Broadcasting Based on Coverage Area and Neighbor Confirmation in Mobile Ad hoc Networks," Proc. of IEEE GLOBECOM'04, 2004..
[9] A. Mohammed, M. Ould-Khaoua, L.M. Mackenzie, C. Perkins, and J. D. Abdulai, "Probabilistic Counter-Based Route Discovery for Mobile Ad Hoc Networks," Proc. of IWCMC'09, pp. 1335-1339, 2009.
[10] W. Peng and X. Lu, "On the Reduction of Broadcast Redundancy in Mobile Ad Hoc Networks," Proc. of ACM MobiHoc'00, pp. 129-130, 2000.
[11] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," *RFC 3561*, 2003.
[12] X. Wu, H. R. Sadjadpour, and J. J. Garcia-Luna-Aceves, "Routing Overhead as A Function of Node Mobility: Molding Structure and Implications on Proactive Routing," Proc. of IEEE MASS'07, pp. 1-9, 2007.
[13] F. Stann, J. Heidemann, R. Shroff, and M. Z. Murtaza, "RBP: Robust Broadcast Propagation in Wireless Networks," Proc. of SenSys'06, pp. 85-98, 2006.
[14] S. Y. Ni, Y. C. Tseng, Y. S. Chen, and J. P. Sheu. "The Broadcast Storm Problem in a Mobile Ad hoc Network," Proc. of ACM/IEEE MobiCom'99, pp. 151-162, 1999.
[15] B. Williams and T. Camp, "Comparison of Broadcasting Techniques for Mobile Ad Hoc Networks," Proc. ACM MobiHoc'02, pp. 194-205, 2002.
[16] F. Xue and P. R. Kumar, "The Number of Neighbors Needed for Connectivity of Wireless Networks," Wireless Networks, vol. 10, issue 2, pp. 169-181, 2004.
[17] X.M. Zhang, E.B. Wang, J.J. Xia, and D. K. Sung, "An Estimated Distance based Routing Protocol for Mobile Ad hoc Networks," IEEE Transactions on Vehicular Technology, vol.60,no.7, pp.3473-3484,Sept. 2011.