International Journal of Engineering Research and Development
ISSN: 2278-067X, Volume 1, Issue 8 (June 2012), PP.41-46
www.ijerd.com

Entry of node in cluster of MANET with Efficient reliable communication

Chandanpreet Kaur[1], Paramjit Singh[2], Ramnik Singh[3]
Asstt.Prof, GIMET Amritsar[1], Asstt.Prof, GIMET Amritsar[2], Asstt.Prof, DAVIET[3], Jalandhar

Abstract—*In this we introduce a decentralized node admission with essential and fundamental security service in mobile ad hoc networks (MANETs). It is required to securely strive with dynamic relationship and topology as well as to bootstrap other important security primitives. Efficient one-to-many dissemination, essential for consensus, now becomes a challenge; enough number of destinations cannot deliver a multicast unless nodes retain the multicast message for exercising opportunistic forwarding. Seeking to keep storage and bandwidth costs low. Trust computations and management are highly challenging issues in MANETs due to computational complexity constraints, and the independent movement of component nodes. Modern routing domains need to maintain a very high level of service availability MANETs are often composed of weak or resource-limited devices; admission must be efficient in terms of computation and communication. We highlight the summary and comparisons of these approaches. We analyze various works on trust dynamics including trust propagation, prediction.*

Index Terms—*MANET, Trust Computations, Propagation, distributed access control, SPBM, ad hoc networks, EGMP.*

I. INTRODUCTION

Distributed collaborations and information sharing are considered to be essential operations in the MANET to achieve the deployment goals such as sensing and event monitoring. Collaboration will be productive only if all participants operate in a trustworthy manner [1]–[3]. MANETs are usually deployed in harsh or uncontrolled environments, thereby heightening the probability of compromises and malfunctioning as there is no centralized control unit to monitor the node operations. These characteristics force a component node to be cautious when collaborating/communicating with other nodes as the behavior of nodes change with time and environmental conditions. Therefore, establishing and quantifying behavior of nodes in the form of trust is essential for ensuring proper operation of MANET. This is particularly important in large scale networks where highly heterogeneous entities participate and high level of collaborations are required e.g., tactical networks with ally nations and social networks [4]. Heterogeneity could be in terms of nodes' operations, sensing capabilities, and other related behavior. Secure node admission in MANETs cannot be performed centrally. This is because a centralized entity is a single point of failure, which also represents an attractive and high-payoff attack target. Moreover, topology changes due to mobility and node outages may cause the central entity to be unreachable and thus unable to perform admission control for the entire network. This motivates us to investigate admission techniques that function in a distributed or decentralized manner. Since our emphasis is on security, the natural technology to consider is threshold cryptography. The notion of threshold cryptography involves distributing cryptographic primitives (such as decryption or digital signatures) in order to secure them against corruption of a certain number of parties, called a threshold. For example, threshold signature scheme [14] allows a group of n parties to distribute the ability to digitally sign messages, such that any t parties can do so jointly, whereas no coalition of less than t parties can sign. Such a threshold signature scheme is resilient against the so-called static adversary who corrupts at most parties in the entire lifetime of the system. Two features of MANETs make decentralized node admission a very challenging problem. First, MANET devices are often limited in terms of computational and battery power. Second, MANET nodes usually function in an asynchronous (on/off) manner, often becoming temporarily unavailable. Therefore, an ideal admission protocol must be efficient in terms of both computation and communication.1 It must also involve minimal (ideally, none at all) interaction among nodes.

Conventional MANET multicast protocols [3]–[8], [28] can be ascribed into two main categories, tree-based and mesh based. However, due to the constant movement as well as frequent network joining and leaving from individual nodes, it is very difficult to maintain the tree structure using these conventional tree-based protocols (e.g., MAODV [3], AMRIS [4], MZRP [5], MZR [28]). The mesh-based protocols (e.g., FGMP [6], Core-Assisted Mesh protocol [7], ODMRP [8]) are proposed to enhance the robustness with the use of redundant paths between the source and the destination pairs. Conventional multicast protocols generally do not have good scalability due to the overhead incurred for route searching, group membership management, and creation and maintenance of the tree/mesh structure over the dynamic MANET. [11]–[14] have been proposed in recent years for more scalable and robust packet transmissions. The existing geographic routing protocols generally assume mobile nodes are aware of their own positions through certain positioning system (e.g., GPS), and a source can obtain the destination position through some type of location service [15] [16]. In [13], an intermediate node makes its forwarding decisions based on the destination position inserted in the packet header by the source and the positions of its one-hop neighbors learned from the periodic beaconing of the neighbors. By default, the packets are greedily forwarded to the neighbor that allows for the greatest geographic progress to the destination[17]. When no such a neighbor exists, perimeter forwarding is used to recover from the local void, where a packet traverses the face of the planar zed local topology sub graph by applying the right-hand rule until the greedy forwarding can be resumed.

A. Efficient geography multicasting protocol.

In this section, we will describe the efficient geography multicasting protocol Group communications is important in supporting multimedia applications. Multicast is an efficient method in implementing the group communications[21]. However, it is challenging to implement efficient and scalable multicast in Mobile Ad hoc Networks (MANET) due to the difficulty in group membership management and multicast packet forwarding over the dynamic topology. We propose a novel Efficient Geographic Multicast Protocol (EGMP). EGMP uses a zone-based structure to implement scalable and efficient group membership management. And a network-range zone-based bi-directional tree is constructed to achieve a more efficient multicast delivery. The position information is used to guide the zone structure building, multicast tree construction and multicast packet forwarding, which efficiently reduces the overhead for route searching and tree structure maintenance. EGMP does not depend on any specific geographic unicast routing protocol. Several methods are assumed to further make the protocol efficient,[23] for example, introducing the concept of zone depth for building an optimal tree structure and combining the location search of group members with the hierarchical group membership management.

EGMP supports scalable and reliable membership management and multicast forwarding through a two-tier *virtual zone- based* structure. At the lower layer, in reference to a pre-determined virtual origin, the nodes in the network self-organize themselves into a set of zones as a leader is elected in a zone to manage the local group membership. At the upper layer, the leader serves as a representative for its zone to join or leave a multicast group as required. [22]As a result, a network-wide zone-based Multicast tree is built. For efficient and reliable management and transmissions, location information will be integrated with the design and used to guide the zone construction, group membership management, multicast tree construction and maintenance, and packet forwarding. The zone-based tree is shared for all the multicast sources of a group. To further reduce the forwarding overhead and delay, EGMP supports bi-directional packet forwarding along the tree structure. That is, instead of sending the packets to the root of the tree first, a source forwards the multicast packets directly along the tree. At the upper layer, the multicast packets will flow along the multicast tree both upstream to the root zone and downstream to the leaf zones of the tree. At the lower layer, when an ontree zone leader receives the packets, it will send them to the group members in its local zone.

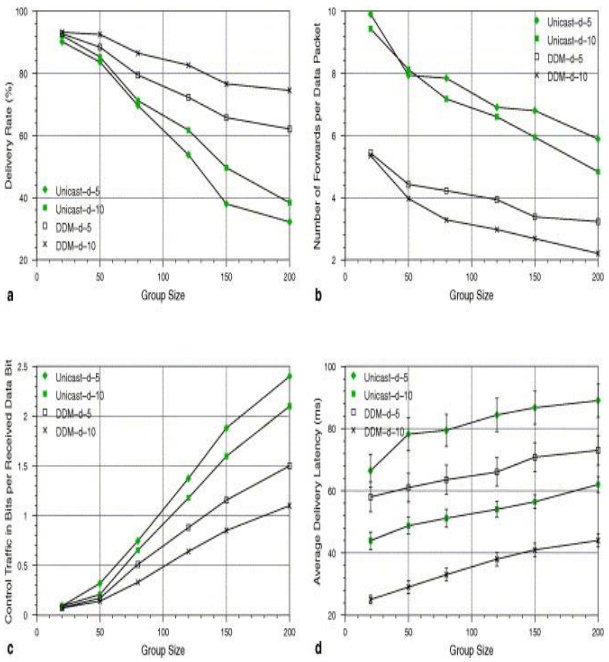

Fig.1 efficient geography multicasting protocol Group communications.

II. RANDOM ORACLE MODEL

Random Oracle Model (ROM) is an effective method for measuring the practical security of cryptograph. In this paper, we try to use it into information hiding system (IHS). Because IHS has its own properties, the ROM must be modified if it is used into IHS. Firstly, we fully discuss why and how to modify each part of ROM respectively. The main changes include:

1) Divide the attacks that HIS may be suffered into two phases and divide the attacks of each phase into several kinds.
2) Distinguish Oracles and Black-boxes clearly.
3) Define Oracle and four Black-boxes that IHS used.
4) Propose the formalized adversary model.
5) Give the definition of judge. Secondly, based on ROM of IHS, the security against known original cover attack.

When prove a protocol's security, we reduce the protocol's security to an Oracle's security. Theoretically, Oracle is a random generator. But as we all know, there has no genuine random generator in practical protocols. In general, Oracle is a basic cryptographic algorithm or a mathematical difficult problem, i.e. the adversary cannot break the Oracle with limited calculating ability at present. Oracle can be considered as the "atomic primitives" of the protocol. Based on the formalized adversary model, we point out that the only method to break the protocol is to break the Oracle. But it is impossible now. So the protocol is secure[24]. When construct a secure protocol, firstly we should figure the protocol using ROM and prove that the formalized protocol is secure. Then we replace oracle by an "appropriately chosen" function *h* to change the formalized protocol into a practical one.

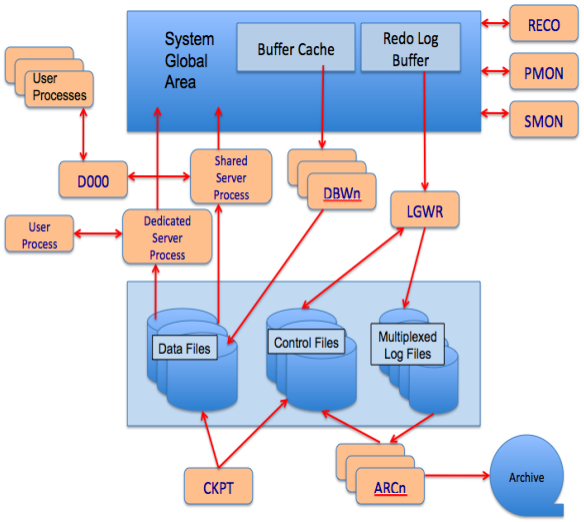

Fig2: Random Oracle Model

III. Effect of the Network Size

To study the scalability of the protocol with network size, we varied the network range from 1500m 1500m to 3900m 3900m. The node density is kept as before, thus the total number of nodes is varied from 156 nodes to 1056 nodes. Since the periodic local and network-wide message flooding in SPBM saturates the memory faster, we run simulations on SPBM with the network size increasing up to only 3300m £ 3300m with 756 nodes. EGMP has a better scalability to the network size than ODMRP and SPBM as demonstrated [22]. The delivery ratios of ODMRP and SPBM drop faster than that of EGMP with the increase of network size. When the network size reaches 3900*m* £ 3900*m* with 1056 nodes, the difference between the delivery ratios of ODMRP and EGMP is more than 55%.

As expected, all the protocols have higher control overheads at a larger network .For ODMRP, more nodes are involved in the periodic JOIN QUERY message flooding[23]. For EGMP, a larger network range leads to longer paths for the control messages at the upper tier. For the geographic based unicast routing, more beacons will be generated with a larger number of network nodes. The control overhead of SPBM, however, is seen to rise much more sharply than those of EGMP and ODMRP, as a result of the increase of quad tree levels in SPBM and the corresponding increase of periodic multi-level message flooding. As the network size increases, due to the longer packet forwarding paths, the total number of data packet transmissions of all the protocols also goes up .Compared to EGMP, SPBM has more than double the packet transmissions in all the network sizes, and the difference becomes more evident at larger network sizes. All three protocols also have longer joining delay when the network size increases[21] .The joining delay of ODMRP is significantly impacted by the network size, as both its periodic network-wide flooding of JOIN QUERY and its broadcast-based packet forwarding will not perform well. More data collisions during the flooding will result in a longer waiting time for a group member to receive the first data packet from the source, and a larger number of packet loss as confirmed by the low delivery ratio. For SPBM, with the increase of the number of the quad-tree levels, the membership change of a node may need to go through more levels to send out leading to a longer joining delay. The joining delay of EGMP only rises slightly, as a new member may need to connect to a farther away tree branch.

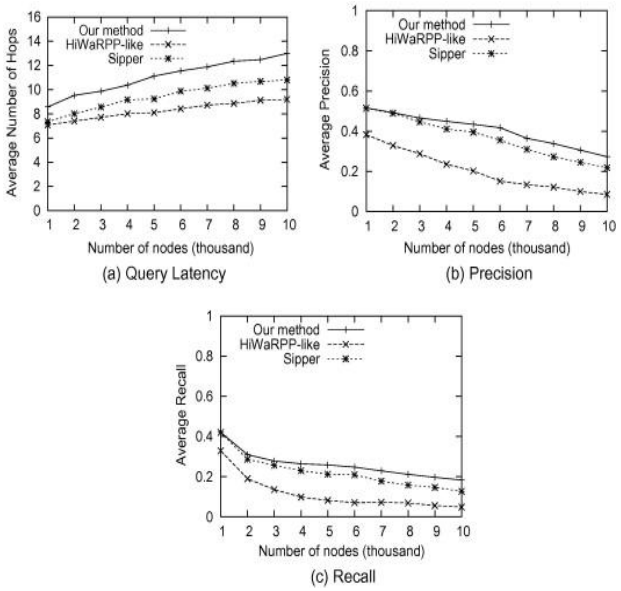

Fig3. Effect of the Network Size with varied range.

A. Generic Admission Control Protocol

The admission control for short-lived MANETs can be realized by only is-suing nodes secret shares. Whereas, for long-lived MANETs, it is also necessary to issue individual node membership corticated. We now discuss the reasoning be-hind this claim. In both long-lived and short-lived MANETs, threshold secret sharing is employed to share the group secret using polynomial of degree (t 1), and every node receives (called a secret share) of the group secret. In long-lived MANETs, nodes need to proactively up-date [11] their secret shares to defend against mobile ad-versifies. This involves updating all coefficients of the secret sharing polynomial, except the constant term (which is the actual group secret), and broadcasting a commitment to the polynomial. However, due to the dynamic and asynchronous nature of the MANETs, it is not always possible for each node to receive updated commitment values. Therefore, the only way to bind the commitment to a node's secret share with the group secret (commitment to which re- mains constant throughout the lifetime and becomes part of the group public key) is by issuing membership corticated to the nodes signed using the group secret[25]. These corticated are then used for authentication and pair wise key establishment purposes. In short-lived MANETs, since there is no need for proactive updates, the polynomial used for sharing the group secret remains constant throughout the lifetime of the MANET and the commitment to this polynomial becomes a part of the group public key. The commitment to each node's secret share is derivable from[25] (and thus automatically bound to) the group public key. Therefore, node membership are not needed in short-lived MANETs. The nodes can use their secret shares (and/or the group public key) for the purpose of secure communication with each other.

We define an admission control mechanism for short lived MANETs as a set of three components:

1. Initialization: The group is initialized by either a trusted dealer or a set of founding members. The dealer or founding members initialize the group by choosing a group secret key, and computing and publishing the corresponding public parameters in the group [16]. The group secret is shared among the founding member(s) in such a way that any set of t members can reconstruct it. The share of the group secret possessed by each member is referred to as its secret share.

2. Admission: A prospective member Mnew who wishes to join the group must be issued its secret share by current member nodes. Mnew initiates the admission protocol by sending a JOIN REQ message to the net- work. A member node, that receives this JOIN REQ message and approves the admission of Mnew, replies, over a secure channel, with a partial secret share (de- rived from its secret share) for Mnew. Once Mnew receives partial secret shares from at least t different nodes, it uses them to compute its secret share. During the above process, a malicious node can easily preclude a prospective node from being admitted by inserting incorrect partial secret shares, i.e., a denial- of-service (DoS) attack. To prevent this, a prospective node must be able to verify the validity of its reconstructed secret share before using them. This feature is called variability in the rest of the paper. Also, when the node detects that its secret share is invalid, it must be able to trace the bogus shares and the malicious node(s) in the MANET. This functionality is provided by the so-called traceability feature. Note that is always required, whereas, traceability is only necessary when a node detects that its reconstructed secrets are not valid.

3. Pair wise Key Establishment: Each node can use its secret share and/or the public parameters to compute pair wise keys with any other node. This allows nodes to securely communicate with each other.

Distributed node admission can be generally described as follows: At some point in time, all current MANET nodes: P1; . . . ; Pn share a secret x in a distributed manner—each Pi has its own secret share xi. The requirement is that any t _ 1 (where t is a security parameter) secret shares do not yield any information about the secret x, whereas any t secret shares completely define x. Now, a new node Pnþ1 needs to be admitted to the group and existing nodes need to supply Pnþ1 with

its secret share such that the new set: x1; x2; . . . ; xn; xnþ1 satisfies the same requirement. Once admitted, they becomes a genuine MANET node (group member).

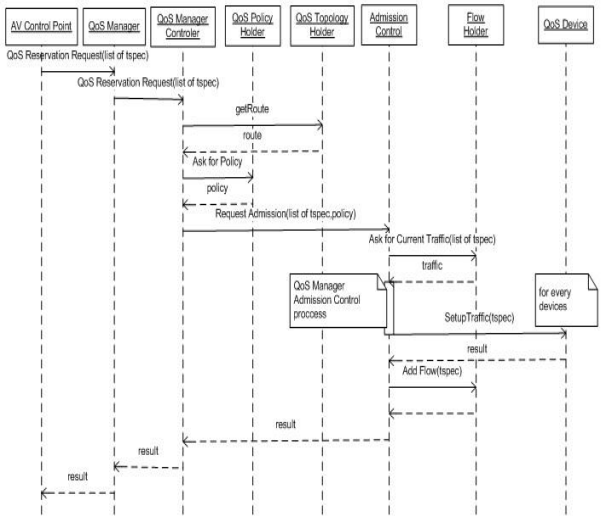

Fig4. The admission control for short-lived MANETs

IV. EFFECT OF NODE DENSITY

Geographic routing is sensitive to the node density and performs better in a dense network. Node density is also closely related to the performance of zone-based protocols. When the node density is low, there will be more empty zones, which will negatively affect the performance[25]. In EGMP, specific design has been made to minimize the impact of empty zone on the performance of multicasting. In geographic routing, the likelihood of using recovery forwarding drops with the increase of network density, and the data packet transmission overhead in SPBM reduces accordingly. However, the transmission overheads of both EGMP and ODMRP increase, and the overhead of ODMRP increases faster[24]. In EGMP, the transmission follows a zone based tree structure. Whenever a data packet reaches an on-tree mzone, it will be forwarded to the leader first, and more on-tree zones will lead to more data packet forwarding and hence a higher packet transmission overhead. In a dense network, the number of empty zones reduces and there is more opportunity for a tree branch to be built between two neighboring zones, which increases the number of on-tree zones and forwarding overhead. The packet transmission overhead of ODMRP goes up because there are more nodes in the forwarding mesh.

V. CONCLUSION

In this survey, we have studied major developments in node admission with efficient and fully no interactive admission technique based on vicariate polynomial secret sharing. We evaluate that our technique compares very favorably to prior results. There is an increasing demand and a big challenge to design more scalable and reliable multicast protocol over a dynamic ad hoc network (MANET). An efficient and scalable geographic multicast protocol, EGMP for MANET The scalability of EGMP is achieved through a two-tier virtual-zone-based structure, which takes advantage of the geometric information to greatly simplify the zone management and packet forwarding. A zone-based bi-directional multicast tree is built at the upper tier for more efficient multicast membership management and data delivery, while the intra-zone management is performed at the lower tier to realize the local membership management. The position information is used in the protocol to guide the zone structure building, multicast tree construction, maintenance, and multicast packet forwarding. Compared to conventional topology based multicast protocols; the use of location information in EGMP significantly reduces the tree construction and maintenance overhead, and enables quicker tree structure adaptation to the network topology change. We also develop a scheme to handle the empty zone problem, which is challenging for the zone-based protocols.

REFERENCES

[1]. K. Barr and K. Asanovic, "Energy Aware Lossless Data Compression," Proc. First ACM Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '03), pp. 231-244, 2003.

[2]. O. Baudron, D. Pointcheval, and J. Stern, "Extended Notions of Security for Multicast Public Key Cryptosystems," Proc. 27th Int'l Colloquium on Automata, Languages and Programming (ICALP '00), pp. 499-511, 2000.

[3]. E. M. Royer and C. E. Perkins. Multicast operation of the ad hoc on-demand distance vector routing protocol. in *Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM)*, August 1999, pp. 207218.

[4]. C. Wu, Y. Tay, and C.-K. Toh. Ad hoc multicast routing protocol utilizing increasing id-numbers (AMRIS) functional specification. *Internet draft*, November 1998.

[5]. X. Zhang and L. Jacob. Multicast zone routing protocol in mobile ad hoc wireless networks. in *Proceedings of Local Computer Networks*, 2003 (LCN 03), October 2003.

[6]. C.-C. Chiang, M. Gerla, and L. Zhang. Forwarding group multicast protocol (FGMP) for multihop mobile wireless networks In *AJ. Cluster Comp, Special Issue on Mobile Computing*, vol. 1, no. 2, pp. 187196, 1998.

[7]. Boneh and Franklin, "Identity-based encryption from the weil pairing," in *Proc. Crypto 2001*, ser. LNCS, vol. 2139. Springer, 2001, pp. 213– 219.

[8]. D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proc. ASIACRYPT*, ser. LNCS, vol. 2248. Springer-Verlag, 2001, pp. 514–532.

[9]. C. Cocks, "An identity based encryption scheme based on quadratic residues," in *IMA: IMA Conference on Cryptography and Coding, LNCS ately (earlier: Cryptography and Coding II, Edited by Chris Mitchell, Clarendon Press, 1992)*, 2001.

[10]. R. Dutta, R. Barua, and P. Sarkar, "Pairing-based cryptographic protocols: A survey," Cryptology ePrint Archive, Report 2004/064, Jun. 24 2004.

[11]. Desmedt and Quisquater, "Public-key systems based on the difficulty of tampering (is there a difference between DES and RSA?) (extended abstract)," in *Proc. Crypto*, 1986.

[12]. H. Tanaka, "A realization scheme for the identity-based cryptosystem," in *Proc. CRYPTO '87*, ser. LNCS, vol. 293. Springer-Verlag, 1988, 16–20 Aug. 1987, pp. 340–349.

[13]. S. Tsujii and T. Itoh, "An ID-based cryptosystem based on the discrete logarithm problem," *IEEE J. Sel. Areas Commun.*, vol. 7, no. 4, May 1989.

[14]. Y. Desmedt and Y. Frankel, "Threshold Cryptosystems," Proc. Ninth Ann. Int'l Cryptology Conf. (CRYPTO '89), pp. 307-315, 1989.

[15]. T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Information Theory, pp. 469-472, 1985.

[16]. P. Feldman, "A Practical Scheme for Non-Interactive Verifiable Secret Sharing," Proc. 28th Ann. Symp. Foundations of Computer Science (FOCS '87), pp. 427-437, 1987.

[17]. E. Fujisaki and T. Okamoto, "Secure Integration of Asymmetric and Symmetric Encryption Schemes," Proc. 19th Ann. Int'l Cryptology Conf. (CRYPTO '99), pp. 537-554, 1999.

[18]. R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Robust Threshold DSS Signatures," Proc. 16th Ann. Int'l Cryptology Conf. (CRYPTO '96), pp. 354-371, 1996.

[19]. R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Secure Distributed Key Generation for Discrete-Log Based Cryptosystems," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT '99), pp. 295-310, 1999.

[20]. S. Goldwasser and S. Micali, "Probabilistic Encryption," J. Computer and System Sciences, vol. 28, pp. 270-299, 1989.

[21]. S. Goldwasser, S. Micali, and R.L. Rivest, "A Paradoxical Solution to the Signature Problem," Proc. 25th Ann. Symp. Foundations of Computer Science (FOCS '84), pp. 441-448, 1984.

[22]. S.-C. M. Woo and S. Singh. Scalable routing protocol for ad hoc networks. In *Wireless Networks*, vol. 7, pp. 513529, 2001.

[23]. A. Ballardie. Core based trees (CBT) multicast routing architecture. In *RFC 2201*, September 1997

[24]. U. P. C. Laboratory. Glomosim. *http://pcl.cs.ucla.edu/projects/glomosim/*.

[25]. J. Yoon, M. Liu, and B. Noble. Random Waypoint Considered Harmful. *Proc. IEEE INFOCOM 03*, 2(4), Apr. 2003.