Secure Data Transition over Multicast Routing in Wireless Mesh network

Adarsh. R, Ganesh Kumar. R, Jitendranath Mungara

ABSTRACT- Multicast routing for wireless mesh networks has focused on metrics that estimate link quality to maximize throughput. Nodes must collaborate in order to compute the path metric and forward data. The assumption that all nodes are honest and behave correctly during metric computation, propagation, and aggregation, as well as during data forwarding, leads to unexpected consequences in adversarial networks where compromised nodes act maliciously.

In high-throughput multicast protocol in wireless mesh networks we identify novel attacks in wireless mesh networks. The attacks exploit the local estimation and global estimation of metric to allow attackers to attract a large amount of traffic. We show that these attacks are very effective against multicast protocols based on high-throughput metrics.

We can say that aggressive path increases attack effectiveness in the absence of defense mechanism. Our approach to defend against the identified attacks combines measurement-based detection and accusation-based reaction techniques. The solution also accommodates transient network variations and is resilient against attempts to exploit the defense mechanism itself. A detailed security analysis of our defense scheme establishes bounds on the impact of attacks. We demonstrate both the attacks and our defense using ODMRP, a representative multicast protocol for wireless mesh networks, and SPP, an adaptation of the well-known ETX unicast metric to the multicast setting.

Keywords – DSA Key Generation, High-Throughput metrics , Wireless mesh Network, Secure Data transition.

I. INTRODUCTION

Wireless mesh networks (WMSs) emerged as a promising technology that offers low-cost high-bandwidth wireless services.

A wireless mesh networks consists of routers, mobile clients through routers. Number of applications envisioned to be deployed in WMSs, such as video conferencing, online gaming, distance learning, web cast and multimedia broadcast. These applications can benefits from the service provided by multicast routing protocol.

In multicast group multicast routing protocols delivers data from source to multiple destinations. Several protocols are proposed to provide multicast services for multi-hop wireless networks.

Manuscript received on August 2012

Adarsh.R, M.Tech, Computer Science and Engineering, CMRIT, Bangalore, India.

Mr Ganesh Kumar R, Assoc Professor and HOD, Dept of ISE, CMRIT, Bangalore, India

Dr. Jitendranath Mungara, Professor and Dean, Dept of CSE and ISE, CMRIT, Bangalore, India.

Initially, these protocols were proposed for mobile ad hoc networks (MANETs) primarily focusing on number of hops (hop count) between the source and receivers as the route selection metric.

The hop count does not maximize throughput as it does not take into account link quantity. Recent protocols focus mainly on quality of link to maximize the throughput; we refer such metric as link-quality or high-throughput metrics, and to protocols using such metric as high-throughput protocols.

In high-throughput multicast protocol, nodes periodically send probes to their neighbors to measure the quality of the links from their neighbors. Cost of the path is calculated by combining its own measured metric of adjacent links with the route cost accumulated on the route discovery packets. The path with best metric is then selected. High-throughput metrics protocol requires the nodes to collaborate in order to deliver the path metrics, thus it assumption that nodes are collaborating and behave correctly during metric computation and propagation. However, this assumption is difficult to guarantee in wireless networks that are vulnerable to attacks coming from both insiders and outsiders. An aggressive path selection may leads to unexpected consequences. Example, adversaries may manipulate the metrics in order to be selected on more paths and to draw mare traffic, creating opportunities for attacks such as data dropping, mesh partitioning, or traffic analysis.

Previous work showed vulnerabilities of unicast routing protocols that use hop count as a metric. Several unicast routing protocols were proposed to cope with outsider or insider attacks. Secure wireless multicast was less studied and focused primarily on tree-based protocols using hop count as a path selection metric.

In this work, we study the security implications of using high-throughput metrics. We focus on multicast in a wireless mesh network environment because it is a representative environment in which high-throughput metrics will be beneficial. Although the attacks we identify can also be conducted in unicast, the multicast setting makes them more effective and, at the same time, more difficult to defend against. We focus on mesh-based multicast protocols as they have the potential to be more resilient to attacks. We use ODMRP as a representative protocol for wireless mesh networks and SPP, a metric based on the well-known ETX unicast metric, as a high-throughput multicast metric. We selected SPP since it was shown to outperform all the other multicast metrics for ODMRP. Our approach to defend against the identified attacks combines measurement-based detection and accusation-based reaction techniques. The solution also

accommodates transient network variations and is resilient against attempts to exploit the defense mechanism itself we limit the number of accusations that can be generated by a node. A detailed security analysis of our defense scheme establishes bounds on the impact of attacks.

II. REVIEW OF LITERATURE

In High-throughput mesh-based multicast routing [2][3] high throughput metrics are used to find the route between source and destination by hop count. In static networks however, this metric was shown to achieve sub-optimal throughput because paths tend to include lossy wireless links [4] [15]. So now focus has shifted toward high-throughput metrics that seek to maximize throughput by selecting paths based on the quality of wireless links(e.g., ETX [4], PP [8] [15], RTT [7]), in such metrics, the quality of the links to/from a node's neighbors is measured by periodic robbing. The metric for an entire path is obtained by aggregating the metrics reported by the nodes on the path.

ETX Metric: The ETX metric [4] was proposed for unicast and estimates the expected number of transmissions needed to successfully deliver a unicast packet over a link, including retransmissions. Each node periodically broadcasts probe packets which include the number of probe packets received from each of its neighbors over a time interval. A pair of neighboring nodes, A and B, estimate the quality of the link A → B by using the formula ETX = 1 / (df×dr), where df and dr are the probabilities that a packet is sent successfully from A to B (forward direction) and from B to A (reverse direction), respectively. The value of ETX for a path of k links between a source S and a receiver R is ETX (s→r) = ∑ (i=1→ k) ETXi, where ETXi is the ETX value of the i-th link on the path; ETX (s→r) estimates the total number of transmissions by all nodes on the path to deliver a packet from a source to a receiver.

SPP metrics- The value of SPP [5] for a path of k links between a source S and a receiver R is SPP (s→r) = Π (i =1→ k) SPPi, where the metric for each link I on the path is SPPi = df and df is defined as in ETX. Unlike in unicast, where a successful transmission over a link depends on the quality of both directions of that link, in multicast only the quality of the forward direction matters because there are no link layer acknowledgments. The quality of a link A → B, as perceived by node B, is SPPi = df and represents the probability that B receives a packet successfully from A over the link A → B. Node B obtains df by counting the probes received from A over a fixed time interval. Also unlike unicast, in which the individual link metrics are summed, in multicast they are multiplied. This reflects the fact that for SPP the probability of a packet being delivered over a path from a source to a receiver is the product of the probabilities that the packet is successfully delivered to each of the intermediate nodes on the path. If any of the intermediate nodes fails to receive the packet, this causes the transmission for the entire route to fail SPP takes values in the interval [0, 1], with higher metric values being better. In particular, SPP = 1 denotes perfect reliability, while SPP = 0 denotes complete unreliability

.

III. HIGH-THROUGHPUT MESH BASED MULTICAST ROUTING

Multicast protocols provide communication from sources to receivers organized in groups by establishing dissemination structures such as trees or meshes, dynamically updated as nodes join or leave the group. Mesh-based multicast protocols build more resilient data paths, but have higher overhead due to redundant retransmissions. We focus on ODMRP as a representative mesh-based multicast protocol for wireless networks. The protocol extension to use a high-throughput metric was first described by Roy [5].We refer to the ODMRP protocol using high-throughput metric as ODMRP-HT in order to distinguish it from the original ODMRP [16] protocol.

ODMRP overview

ODMRP is an on-demand multicast routing protocol [16] for multi-hop wireless networks, Nodes are added to the mesh through a route selection and activation protocol. The source periodically recreates the mesh by flooding a JOIN QUERY message in the network in order to refresh the membership information and update the routes. JOIN QUERY messages are flooded using a basic flood suppression mechanism, in which nodes only process the first received copy of a flooded message.

When a receiver node gets a JOIN QUERY message, it activates the path from itself to the source by constructing and broadcasting a JOIN REPLY message that contains entries for each multicast group it wants to join; each entry has a next hop field filled with the corresponding upstream node. When an intermediate node receives a JOIN REPLY message, it knows whether it is on the path to the source or not, by checking if the next hop field of any of the entries in the message matches its own identifier. If so, it makes itself a node part of the mesh and creates and broadcasts a new JOIN REPLY built upon the matched entries. Once the JOIN REPLY messages reach the source, the multicast receivers become connected to the source through a mesh of nodes which ensures the delivery of multicast data. While a node is in the FORWARDING GROUP, it rebroadcasts any non-duplicate multicast data packets that it receives. ODMRP takes a "soft state" approach in that node put a minimal effort to maintain the mesh. Nodes are no need send message to leave the group, if nodes didn't replayed to forward message then we can assume that nodes are leaving from the group. If the forward node status is not updated then nodes are not able to participate in the forward-group.

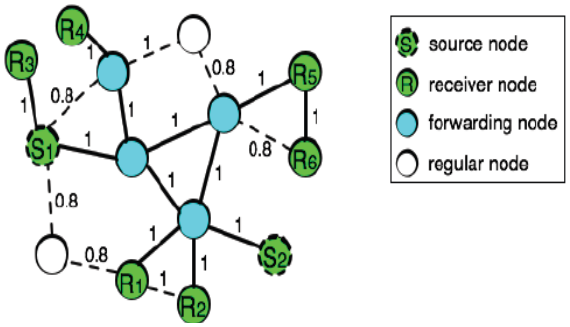
ODMRP-HT

Protocol that enhances ODMRP with high-throughput metrics. The main differences between ODMRP-HT and ODMRP are:
(1) Instead of selecting routes based on minimum delay (which results in choosing the fastest routes), ODMRP-HT selects routes based on a link-quality metric, and
(2) ODMRPHT uses a weighted flood suppression mechanism to flood JOIN QUERY messages instead of basic flood suppression.

Attacks against high-throughput multicast and their Impact

The attacks exploit vulnerabilities introduced by the use of high-throughput metrics. They require little resource from the attacker, but can cause severe damage to the performance of the multicast protocol.

Fig. 1: An example of ODMRP-HT meshes creation for a multicast group with 2 sources (S1, S2) and 6 receivers (R1. R6). The label on link represents the value of the link's SPP metric.



Adversarial Model:

Malicious nodes may exhibit Byzantine behavior; either alone or in collusion with other malicious nodes, refers to any arbitrary action by authenticated nodes deviating from protocol specification as Byzantine behavior, and to such an adversary as a Byzantine adversary. Examples of Byzantine behavior include: Dropping, injecting, modifying, replaying, or rushing packets, and creating wormholes. We do not consider the Sybil attack, which can be addressed using techniques, complementary to our routing protocol.

Attack Goals:

The two main attack targets that allow the attacker to achieve this goal are the path establishment and data forwarding phases of the protocol. Path establishment attacks prevent receivers from connecting to multicast sources. In ODMRP-HT, since each receiver only activates a single path to each source, an attacker lying on that path can prevent path establishment by dropping the JOIN REPLY message. Data forwarding attacks disrupt the routing service by dropping data packets. In both cases, the attack effectiveness is directly related to the attackers' ability to control route selection and to be selected on routes. Traditionally, such ability can be achieved via wireless-specific attacks such as rushing and wormholes

Metric Manipulation Attacks:

For an attacker to increase its chances of being selected in the FORWARDING GROUP is to advertise artificially good metrics for routes to the source. Adversaries can execute two types of metric manipulation attacks: local metric manipulation (LMM) and global metric manipulation (GMM).

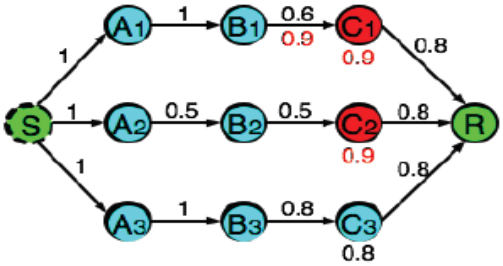


Fig 2: Metric manipulation attack during the propagation of the flood packet from the source S to receiver R. A label above a link is the link's real SPP metric; a label below a link is the link's metric falsely claimed by a node executing a LMM attack; a label below a node is the route metric advertised by the node.

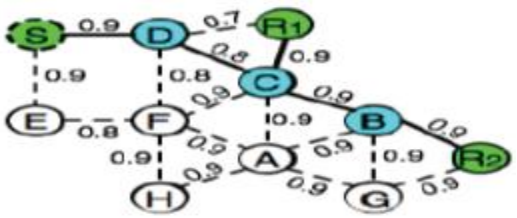
Local Metric Manipulation (LMM) Attacks: An adversarial node artificially increases the quality of its adjacent links, distorting the neighbors' perception about these links. The falsely advertised "high-quality" links will be preferred to select the route so, malicious nodes have better chances to be included on forward group. A node can claim a false value for the quality of the links towards itself.

Global Metric Manipulation (GMM) Attacks: In a GMM attack, a malicious node arbitrarily changes the value of the route metric accumulated in the flood packet, before rebroadcast this packet. A GMM attack allows a node to manipulate not only its own contribution to the path metric, but also the contributions of previous nodes that were accumulated in the path metric.

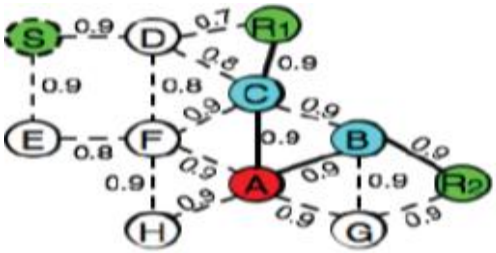
Impact of Metric Manipulation Attacks on Routing:

The attacks allow attackers to attract and control traffic. the epidemic nature of metric derivation causes an epidemic attack propagation, which "poisons" the metrics of many nodes in the network.

When no attackers are present (Fig. 3(a)), nodes B, C and D are activated as part of the FORWARDING GROUP. Consider that node A executes a metric manipulation attack (Fig.3(b)): Upon receiving the JOIN QUERY, node A changes the metric and advertises a perfect metric with value 1. Consequently, both receivers R1 and R2 are "attracted" to it and only nodes B and C will be selected as part of the FORWARDING GROUP. The net effect is that both R1 and R2 are denied service since they do not have a path to the source. The false metric advertisement by node A also poisons the metrics of many nodes in the network. For example, node C derives an incorrect metric of 0.9, and then propagates it to its neighbors, causing them to derive an incorrect metric as well.



(A)Benign Case



(B) Attack Case

Fig.3: Metric manipulation attack in a network with one source (S), two receivers (R1, R2) and one attacker (A).

For example, even if A's neighbors are able to detect A is an attacker, they cannot rely on the metric to find a new route to the source. Indeed, if node C detects that A is malicious, it can try to activate nodes F or B, which advertised the second best metric; however, routes through either F or B lead back to the attacker. The problem stems from the fact that the metric cannot be relied upon and nodes do not know the right direction to "break free" from the attraction of A.

IV. SECURE DATA TRANSTITION OVER MULTICAST ROUTING

In this section, we present our secure multicast routing protocol (S-ODMRP) that accommodates high-throughput metrics. In the Fig 4 shows the architecture diagram in which server sends the 'req for the connection' to router if the connection is not confirmed then server sends the 'req for connection' again. If the connection is confirmed then the router sends the data to the clients connected to router, if the data is not received correctly then clients can send the request to send the data again. Before sending the data from server to client through router data is signed by using DSA KEY generation.

Key generation has carried out by choice of algorithm parameters which may be shared between different users of the system: Choose an approved cryptographic hash function H. In the original DSS, H was always SHA-1, but the stronger SHA-2 hash functions are approved for use in the current DSS. The hash output may be truncated to the size of a key pair. Decide on a key length L and N. This is the primary measure of the cryptographic strength of the key. The original DSS constrained L to be a multiple of 64 between 512 and 1024 (inclusive). Recommends lengths of 2048 (or 3072) for keys with security lifetimes extending beyond 2010 (or 2030), using correspondingly longer N.[3] specifies L and N length pairs of (1024,160), (2048,224), (2048,256), and (3072,256).

Once the key is generated we need to sign in on each packet, so that all the packets which are sending from server to client had signed. Digital signatures employ a type of asymmetric cryptography. For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type.

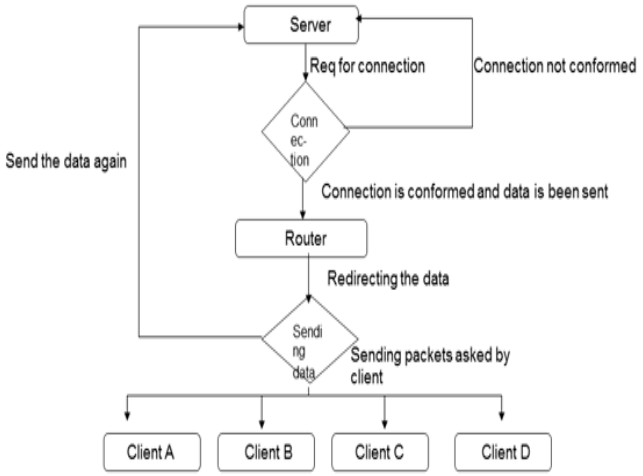


Fig 4.Architecture diagram

Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless.

After packets are received at client, clients need to verify the sign on each packet to verify each packet are received correctly or not. Signature verification may be performed by any party (i.e., the signatory, the intended recipient or any other party) using the signatory's public key. A signatory may wish to verify that the computed signature is correct, perhaps before sending the signed message to the intended recipient. The intended recipient (or any other party) verifies the signature to determine its authenticity. Prior to verifying the signature of a signed message, the domain parameters, and the claimed signatory's public key and identity shall be made available to the verifier in an authenticated manner. The public key may, for example, be obtained in the form of a certificate signed by a trusted entity (e.g., a Certification Authority) or in a face-to-face meeting with the public key owner.

S-ODMRP Overview

Our approach relies on the observation that regardless of the attack strategy, attackers do not affect the multicast protocol unless they cause a drop in the packet delivery ratio (PDR).In previous secure wireless was less studied [13] [14], We adopt a reactive approach in which attacker nodes are detected through a measurement-based detection protocol component, and then isolated through an accusation-based reaction protocol component. We next describe these two components.

Measurement-based attack detection: Whether by packet dropping alone or by combining it with metric manipulation to attract routes, the effect of an attack is that data is not delivered at a rate consistent with the advertised path quality. We propose a generic attack detection strategy that relies on the ability of honest nodes to detect the discrepancy between the expected PDR (ePDR) and the perceived PDR (pPDR). A node can estimate the ePDR of a route from the value of the metric for that route2; the node can determine the pPDR for a route by measuring the rate at which it receives data packets from its upstream on that route3. Both FORWARDING GROUP nodes and receiver nodes monitor the pPDR of their upstream node. If ePDR−pPDR for a route becomes larger than a detection threshold, then nodes suspect that the route is under attack because the route failed to deliver data at a rate consistent with its claimed quality4.

Accusation-based attack reaction: We use a controlled accusation mechanism in which a node, on detecting malicious behavior, temporarily accuses the suspected node by flooding in the network an ACCUSATION message containing its own identity (the accuser node) and the identity of the accused node, as well as the duration of the accusation. As long as the accusation is valid, metrics advertised by an accused node will be ignored and the node will not be selected as part of the FORWARDING GROUP. This strategy also successfully handles attacks against path establishment. From the downstream node point of view, the dropping of a JOIN REPLY message causes exactly the same effect as the attacker dropping all data packets, thus the downstream nodes will react and accuse the attacker.

To prevent the abuse of the accusation mechanism by attackers, a node is not allowed to issue a new accusation before its previously issued accusation expires. Accused nodes can still act as receivers even though they are excluded from the FORWARDING GROUP. We use a temporary accusation strategy to cope with transient network variations: The accusation duration is calculated proportional to the observed discrepancy between ePDR and pPDR, so that accusations caused by metric inflation and malicious data dropping last longer, while accusations caused by transient network variations last shorter. Finally, to address the metric poisoning effect caused by metric manipulation attacks, the metric in the entire network is refreshed shortly after attack detection. In S-ODMRP, the metric refreshment is achieved automatically through the Periodic JOIN QUERY messages.

V. GENERALIZATION OF S-ODMRP

Although we have described our defense scheme for high throughput multicast protocols using the SPP metric, our defense scheme can be generalized to other high throughput metrics and other high performance multicast protocols.

Application to Other High Throughput Metrics: S-ODMRP relies on the ability to derive an estimated PDR (ePDR) from the metric. For the SPP metric, the derivation is straightforward: The estimated PDR equals the SPP metric value. What about other high throughput metrics? We first observe that the goal of a high throughput multicast protocol is to achieve a high PDR, hence a good metric should reflect the PDR to some extent. For metrics that have a clear connection with PDR, one approach is to define a mapping function that translates metrics to PDR. The data delivery path is determined based on the value of metric. The data delivery path selection algorithm should be enhanced to also consider the consistency between PDR and metric in the received metric tuple, such that nodes advertising low PDR but high metric are avoided.

Application to Other Multicast Protocols: Our defense strategy to rely on measurement-based detection and accusation-based reaction generalizes to a class of high performance multicast protocols that exhibit the following characteristics:

• Path selection is based on the greedy approach of selecting path with best metric.

• An estimation of the target performance metric can be derived from the path metric.

• There exists an efficient metric refreshment protocol that allows nodes to obtain correct metrics for attack recovery. Such metric refreshment can be easily achieved by flooding of a new metric establishment message.

As an example, consider a multicast protocol that aims to achieve low latency communication. Then, a good path metric is the latency of a node to the source, which can be derived and propagated in the same fashion as the SPP metric. Each node greedily selects the neighbor with the minimum latency metric to be on the path. In such a protocol, an attacker can disrupt the protocol by advertising a low latency metric to attract many nodes, but intentionally delays packets.

VI. CONCLUSION

We considered the security implication of using high throughput metrics in multicast protocols in wireless mesh networks. In particular, we identified metric manipulation attacks that can inflict significant damage on the network. The attacks not only have a direct impact on the multicast service, but also raise additional challenges in defending against them due to their metric poisoning effect.

We overcome the challenges with our novel defense scheme that combines measurement-based attack detection and accusation-based reaction. Our defense also copes with transient network variations and malicious attempts to attack the network indirectly by exploiting the defense itself. We demonstrate through experiments that our defense is effective against the identified attacks, resilient to malicious exploitations, and imposes a small overhead.

VII. FUTURE WORK

By Secure Data Transition over Multicast in Wireless Mesh Network We can send the data securely by transmitting data over all the nodes in network, Instead of sending data to all nodes in the network we can send data to neighbor's node, so it minimizes the time taken to select the path.

We can use the Cloud technology to store the data, so that all the server, router, clients connected in the network can easily view the correct data with less time and it minimizes the memory required to store data.

REFERENCES

1. J. Dong, R. Curtmola, and C. Nita-Rotaru, "On the pitfalls of using highthroughput multicast metrics in adversarial wireless mesh networks," in Proc. of IEEE SECON '08, 2008.
2. Y. B. Ko and N. H. Vaidya, "Flooding-based geocasting protocols for mobile ad hoc networks," Mob. Netw. Appl., vol. 7, no. 6, 2002.
3. R. Chandra, V. Ramasubramanian, and K. Birman, "Anonymous gossip: Improving multicast reliability in mobile ad-hoc networks," in Proc. Of ICDCS, 2001.
4. D. S. J. D. Couto, D. Aguayo, J. C. Bicket, and R. Morris, "A highthroughput path metric for multi-hop wireless routing," in Proc. Of MOBICOM '03. ACM, 2003, pp. 134–146.
5. S. Roy, D. Koutsonikolas, S. Das, and C. Hu, "High-throughput multicast routing metrics in wireless mesh networks," in Proc. of ICDCS '06, 2006.
6. A. Chen, D. Lee, G. Chandrasekaran, and P. Sinha, "HIMAC: High throughput MAC layer multicasting in wireless networks," in Proc. Of Mobile Adhoc and Sensor Systems (MASS '06), October 2006.
7. A. Adya, P. Bahl, J. Padhye, A. Wolman, and L. Zhou, "A multi-radio unification protocol for ieee 802.11 wireless networks," in Proc. Of BroadNets '04, 2004.
8. S. Keshav, "A control-theoretic approach to flow control," Proc. of the Conference on Communications Architecture and Protocols, 1993.
9. P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hocnetworks," in Proc. of CNDS, January 2002, pp. 27–31.
10. Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. of WMCSA, June 2002.
11. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in Proc. of MOBICOM, 2002.
12. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. of MOBICOM, August 2000.
13. S. Roy, V. G. Addada, S. Setia, and S. Jajodia, "Securing MAODV: Attacks and countermeasures," in Proc. of SECON '05. IEEE, 2005.
14. R. Curtmola and C. Nita-Rotaru, "BSMR: Byzantine-resilient secure multicast routing in multi-hop wireless networks," in Proc. of IEEE SECON '07, June 2007.
15. R. Draves, J. Padhye, and B. Zill, "Comparison of routing metrics for static multi-hop wireless networks," in Proc. of SIGCOMM '04, 2004.
16. S. Roy, D. Koutsonikolas, S. Das, and C. Hu, "High-throughput multicast routing metrics in wireless mesh networks," Elsevier Ad Hoc Networks, 2007.