# PACKET DROP ATTACK: A SERIOUS THREAT TO OPERATIONAL MOBILE AD HOC NETWORKS

Venkatesan Balakrishnan and Vijay Varadharajan
Information and Networked System Security Research Group
Department of Computing
Macquarie University
Sydney, Australia
{venkat,vijay}@ics.mq.edu.au

**ABSTRACT**
In recent years the widespread availability of wireless communications, mobile computing and handheld devices has led to the growth and significance of wireless mobile ad hoc networks. Security issues are paramount in such networks even more so than in wired networks. Though there have been many works in the recent years on secure routing protocols, the "Packet Drop Attack" amongst the nodes is not adequately addressed. In this paper, we analyze a class of secure routing protocols such as SAODV, ARAN and Security Aware Ad Hoc Routing to show how they are vulnerable to packet drop attacks. We also investigate another class of secure routing protocols such as CONFIDANT that cater to defend packet drop attacks but fail due to not having well-defined trust model. The detail study of packet drop events in these protocols leads us to propose a defense-in-depth strategy to secure mobile ad hoc networks through the integration of three layers -- prevention layer (based on cryptographic techniques), detection-reaction layer (based on monitoring technique) and enforcement layer (based on obligations).

**KEY WORDS**
Security, Routing, Mobile Ad hoc Networks, Packet Drop Attack

## 1. Introduction

The ability to establish communication without an infrastructure and the capacity to communicate beyond the node's wireless transmission range embarks Mobile Ad hoc Networks (MANET) as the deployment ground for various fields such as wireless sensor networks, ubiquitous networks and peer-to-peer networks. Implicitly, the low cost, undemanding maintenance and simplicity acknowledges mobile wireless networks as an alternative to the existing wired networks. The proliferation of communication devices and the evolution of technology confirm that it is the tool, which can turn the existing computing space into smart space.

Though MANET promises to be the operational base for most of applications, security issues are paramount in such networks even more so than in wired networks. The fundamental problem in mobile ad hoc networks is the lack of consistency to deliver information to the intended node. Furthermore, the environment is not conducive to the assumption of a centralized trusted authority due to the dynamic nature of the environment. At the same time, the need to address the availability of services irrespective of the mobility creates serious challenges in the design. Additionally, the feasibility of nodes to operate at promiscuous mode, especially in the shared wireless medium raises serious concern on the confidentiality of the transmitted messages. Lastly, the resource-constrained environment narrows the choice of techniques deployed. With all these factors put together, the designer is not only forced to model secure primitives for routing but also forced to handle fault tolerant mechanisms to stabilize the model, because it is not always clear whether a route is unavailable due to an attack or node's mobility or congestion.

In this paper, we address the "Packet Drop Attack", which is a serious threat to operational mobile ad hoc networks. Though there have been many works in the recent years on secure routing protocols, the packet drop attack amongst the nodes is not adequately addressed. We analyze a range of secure routing protocols to show how they are vulnerable to packet drop attacks. These protocols are static and employ cryptographic techniques to prevent the basic operation of the protocol and hence inherently they fall short in handling the dynamic changes. We also investigate another class of secure routing protocols that cater reputation oriented trust models to defend packet drops but fail due to not having cryptographic mechanisms and well formalized trust models. These protocols deploy neighborhood monitoring to capture the dynamic events in the environment but miss to meet the requirements as trust management in MANETs has not been well studied yet [1]. The detail study on the gravity of packet drop event (which may even prevent the network to emerge and operate at extreme cases) leads us to propose a defense-in-depth

strategy to secure mobile ad hoc networks through the integration of three layer -- prevention layer (based on cryptographic techniques), detection-reaction layer (based on monitoring and trust management) and enforcement layer (based on obligations). The acumen that a packet might be dropped by a malicious node or a benign node due to various reasons urged us to propose the design, which includes an additional layer – enforcement layer, apart from the existing layers (prevention layer and detection-reaction layer), so that the nodes are obligated towards the basic operation of the network subject to its inherent resources.

In the following section, we list the distinguished routing attacks in MANET. Section 3, deals with the operation of the basic on-demand routing protocols. The seriousness of packet drop attack is explained in section 4, followed by the detailed study of secure routing protocols in section 5. Section 6 necessitates the need to include an additional layer with the existing layers to defend packet drop event and then we conclude the paper.

## 2. Routing Attacks in MANET

MANETs are vulnerable to a range of attacks from route disruption to resource exhaustion. Though the attacks differ grounded on the mode of execution, they are predominantly derived from three basic active attack approaches. Here, we ignore the attacks raised through the passive approaches.

Basic Active Attack Approaches,

- Modification Approach: The intruder alters the contents of the control message transmitted in its environment and replays the altered content back to the environment to cause malicious effect.
- Fabrication Approach: The attacker creates and transmits malicious control messages to the environment aimed to destruct the basic routing operation or destroy other's resources.
- Interruption Approach: The malicious node performs specific actions to interrupt the normal operation of the network without modifying or fabricating the control messages.

Attacks classified based on the mode of execution,

- Routing loop attack [2], where a malicious node modifies the route header during the route discovery phase, so that the intermediate nodes waste their resources in routing the packets in a loop fashion.
- Blackhole attack [3] attracts all the packets towards it by altering the routing information and then drops those packets. Grayhole attack is a specialized version of a blackhole attack, where the malicious node selectively drops packets.
- Flooding attacks [4] causes the intermediate nodes to burn their resources in processing the incoming flooded-falsified routing information and in some cases blows out the routing table due to overflow.
- Spoofing attack [5], one of the most vulnerable attacks, allows the node to become an authorized entity in the network and permits to take advantage of the authorized services.
- Detour attack [3] accounts for the packets to be routed along the suboptimal path to prevent one set of nodes from reaching another. In gratuitous attack, an attacker modifies the route information to appear long, so that it is not routed through the attacker.
- Rushing attack [6] arises due to the route suppression technique adopted in routing protocols such as Ad hoc On Demand Vector Routing Protocol (AODV), where the malicious node disseminates the ROUTE REQUEST quickly throughout the network before the legitimate ROUTE REQUEST is forwarded.
- Blackmail attack [5] incurs due to lack of authenticity and it grants provision for any node to corrupt other node's legitimate information.
- Wormhole attacks [7] are nothing but tunneling attacks, preventing nodes from discovering successful routes.
- Route salvaging attack [2] is significant in nodes deploying routing protocols like AODV. This enables malicious nodes to invoke falsified route salvations in order to diminish the network resources.
- Falsified Route Error Generation attack [1] causes the source node to re-initiate route discovery through the generation of false control messages. On other hand, "Valid Route Error Suppression" arises due to the suppression of valid route errors when the link is actually broken.

Either internal or external attackers can launch these attacks; the internal attackers in most cases launch the attacks via the compromised nodes, taking the advantage of the authorized entity in the network.

## 3. Primary Routing Protocols in MANET

Though there are multiple classes of routing protocols in MANET to achieve multi-hop routing between any two nodes, we choose source-initiated on-demand routing protocols for our study. Among them, we consider only the secure routing mechanisms built on Dynamic Source Routing (DSR) protocol [8] and Ad-hoc On Demand Vector Routing (AODV) protocol [9]. Reasons to consider them are due to their efficiency, dynamic nature, wider acceptance and the consideration for standardization. We briefly describe DSR's operation for completion and address the inherent weaknesses persisting within on-demand routing protocols.

DSR is the acronym for "Dynamic Source Routing" protocol, where each node to communicate with any other node in the network, initially checks its route cache for the route information corresponding to the intended

destination prior sending a packet to the destination. On failure to find a route from the cache, it initiates route discovery by broadcasting ROUTE REQUEST packet to all its neighbors, who in turn broadcast the ROUTE REQUEST to its neighbors. The ROUTE REQUEST collects the list of nodes on its path before it reaches the destination or the node, which has a valid source route to the destination. If an intermediate node has a valid route to the destination, it transmits ROUTE REPLY back to the source; this can be achieved by inverse routing or by initiating another route discovery towards the source. In case of broken link or error, the route maintenance initiates a ROUTE ERROR to the source. Though it can handle unidirectional links and multiple routes, it occupies a large bandwidth due to the source routing.

On contrary, AODV takes advantage of the hop count, thereby reducing the network bandwidth overhead. It is scalable due to the usage of two addresses and hop count, but turns out to be worse in the case of asymmetric links, where DSR takes the lead.

The concept of changing the internal states of each node, based on the information routed through it, raises a serious issue because the receiving node does not have provisions to check the authenticity of the information before those changes are reflected. Moreover, the route information is judged purely based on the metrics, which requires addition of extra mechanisms to secure them. Apart from the well-known fact that the initial development of basic on-demand routing protocols did not consider security during its design, we can see that the design had placed a strong implicit assumption that all the participants by default will forward the packets received from other nodes.

## 4. Packet Drop Attack

From the analysis of basic on-demand routing protocol's operation in section 3, it is inherently understandable that the design assumes the participants to forward others packets, which is an unrealistic anticipation in an independent network like MANET. The consequence of not forwarding others packets or dropping others packets prevents any kind of communication to be established in the network. Hence given a choice between the necessity to secure services or to ensure basic functioning of the network, intrinsically the choice falls for the latter. Therefore, the need to address the packet dropping event takes higher priority for the mobile ad hoc networks to emerge and operate successfully.

A packet may be dropped under various reasons, which in turn can be grouped into the following categories,

1) Unsteadiness of the medium,
   - A packet may be dropped due to contention in the medium
   - A packet may be dropped due to congestion and corruption in the medium
   - A packet may be dropped due to broken link

2) Genuineness of the node,
   - A packet may be dropped due to overflow of the transmission queue
   - A packet may be dropped due to lack of energy resources

3) Selfishness of the node,
   - A packet may be dropped due to the selfishness of a node to save its resources

4) Maliciousness of the node,
   - A packet may be dropped due to the malignant act of a malicious node

The unsteadiness of the medium generally causes errors in the packet, which forces the benign node to drop the packet even if the node aspires to forward it. On other hand, a genuine node with zero options may drop the packets when it runs out its resources. Though a packet may be dropped in the similar manner by a selfish or a malicious node, they distinctly differ from the others because the packets are dropped intentionally. From the above examination, it is obvious that the intentional packet drop events have to be tackled, which we generalize as "Packet Drop Attack", contrast to the accidental packet drop events. However, we envisage that the proposal should also encompass mechanisms to detect the accidental packet drops and adjust dynamically according to them, thereby enhancing the basic operation of the protocol. In the following section, we investigate a set of secure routing protocols to understand the seriousness of packet drop attack.

## 5. Secure Routing Protocols in MANET

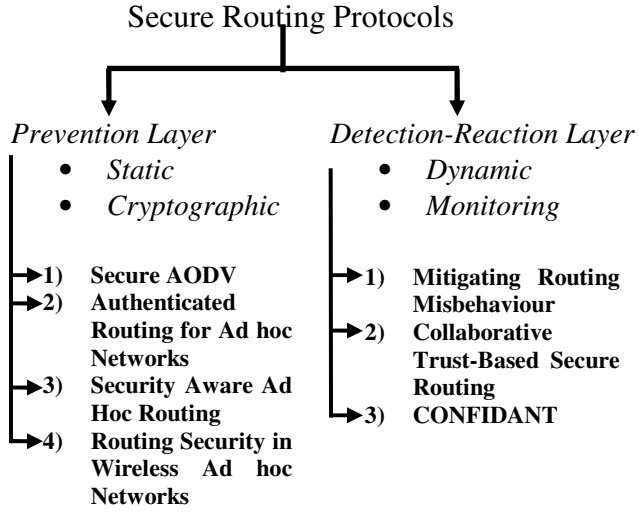


Figure 1 Taxonomy of Secure Routing Protocols – Examined for Packet Drop Attack

We group the secure routing protocols into two classes:

- Protocols that deploy cryptographic techniques to secure the routing usually remain static during the operation. They are actually classified under the prevention layer.
- Protocols that deploy monitoring technique capture the dynamic events to enhance the protection of the basic operation. They are actually referred as detection-reaction layer in the defense-in-depth security design [1].

In the following section, we present the strengths and weaknesses of the approaches through a detailed study. We assume that the reader has basic knowledge in the working of the protocols stated below.

## 5.1 Protocols Deploying Cryptographic Techniques

### 5.1.1 SAODV

Secure AODV (SAODV) [10][11][12] employs asymmetric mechanisms to achieve authentication, integrity, confidentiality and non-repudiation. It is assumed that the public key should come with the IP address of the node and the network leader's IP address as the mask address, to avoid impersonation attacks. The source with the help of signature key pair signs the mutable fields of the RREQ and in the case of RREP it is signed by destination. Hence both can verify and authenticate each other using their public keys. The signature contains the seed of the hash chain embedded within it, which secures the hop count. For each hop the intermediate nodes increases the hop by hashing the previous hash count value. The one-way nature of the hash chain prevents the reduction of the hop count.

Certificates bounded with IP addresses are unrealistic, as nodes may be assigned with dynamic IP addresses. Deployment of asymmetric key techniques not only raise issues like incremental deployment and key revocation but also consumes huge resource in an energy-constrained environment due to the high processing overhead at each node for every request. SAODV is still prone to the same distance fraud [6], where the forwarding node fails to increment the route metric, as there is no enforcement to do so. Moreover, SAODV never considers the misbehaving detection methods and also does not take any attempt to prevent DOS attacks because it assumes that DOS attacks are more predominant and restricted to physical layer; this is not true, for example colluding malicious nodes can drop packets during route discovery phase.

### 5.1.2 ARAN

In Authenticated Routing for Ad hoc Networks (ARAN) [2], the certificates signed by the certificate authority, associate each node's IP address with its public key. In a route request, the source includes its certificate, target's IP address, nonce, and timestamp for freshness and authenticity. An intermediate node removes the previous forwarding node's signature and certificate (except the source node's signature and certificate), signs the route request and includes its own certificate. Similarly, when any node receives the route reply, it removes the signature and certificate of the previous hop from whom the route reply was received (except the signature and certificate of target node, which is actually the destination node for the route request), signs the original reply from the target and includes its own certificate. The intermediate node establishes an entry in the routing table for the source or the target, when it receives the request or reply respectively. Route request and route reply are similar except that the request is a broadcast and the reply is a unicast. Due to the heavy computation involved with the certificates, the ARAN system is vulnerable to many DOS attacks. Even when there is no malicious node, the load levied on the legitimate intermediate nodes force them to drop the packets in order to conserve their resources.

### 5.1.3 Security Aware Ad Hoc Routing

Consider now the situation where the nodes are grouped based on the trust level [13][14][15] and the source node initiating the route request suggests that only nodes satisfying the minimum security level can take part in the route discovery and other nodes that do not have the necessary trust level have to drop the request packets. To secure and differentiate each level, a level is assumed to share a key, which can also participate with lower levels but not with higher levels. A malicious node at a particular level can launch any attack at its level or at lower levels. Moreover, it fails to address the global secure routing problem and concentrates on secure routing in a context, where nodes of a certain group are assumed to be trustworthy. The fixed assignment of trust levels further worsens the design. In our context of packet drop attack, within a trust level, any malicious node or legitimate node, which aims at saving its resource can successfully drop packets without being noticed and can continue to utilize the service from other nodes for forwarding its own packets.

### 5.1.4 Routing Security in Wireless Ad hoc Networks

Hongmei Deng et al. [16] propose a simple solution to address the blackhole attack. In general, the provision to allow intermediate nodes to send ROUTE REPLY on behalf of the destination to reduce the delay, if they have a valid route to destination, always creates an opportunity for the blackhole attack. The proposed solution crosschecks whether the ROUTE REPLY from intermediate node is valid or not by verifying the existence of the route between the intermediate node and

the destination at two stages. Whenever the intermediate node replies with a ROUTE REPLY, if it has a valid route to the destination, it has to send its *next hop* information along with it. The source then verifies the route between the intermediate node and the destination by initiating *Further Request* to the *next hop* node. To avoid recursion, only the *next hop* node is permitted to respond via *Further Reply* with the *check result* field containing the result of the query. If the response confirms that the *next hop* node lies between the intermediate node and the destination, then the route through the intermediate node is chosen. On the contrary, if the response informs that *next hop* node is not in-between the intermediate node and the destination, but has a valid route to the destination, then the ROUTE REPLY from the *next hop* is chosen. However, if the above two possibilities are unsuccessful, then the source initiates a new route discovery.

The approach is an exception to this section because it neither performs cryptographic technique nor monitoring technique. However, it is a static approach to defend the blackhole attack. The method lays a strong assumption that there are no colluding attacks. Even if the assumption is true, presence of non-colluding multiple malicious nodes adjacent to each other will indirectly give the opportunity for the adjacent malicious node to launch blackhole attack.

#### 5.1.5 Discussion

In general, approaches levying heavy computations at intermediate nodes are at the risk of motivating selfish nodes. The selfish nodes may easily achieve their goal by simply boycotting others' route discovery, where the node initiating route request may be forced to perform many iterations of route discovery phase, draining its resources futilely. The severity of selfishness or greediness is to the extent that the operation of the network can come to stand still even in the absence of the malicious nodes. Hence, to attract them, it becomes essential to reduce or completely eliminate heavy computations at intermediate nodes. On other hand, the heavy computation levied at intermediate nodes also decreases the average network's lifetime significantly. To conclude, the approaches deploying cryptographic techniques alone cannot defend packet drop attack because they fail to observe the dynamic changes in the environment, which is required to identify the intentional packet drops from genuine accidental packet drops.

### 5.2 Protocols Deploying Monitoring Techniques

#### 5.2.1 Mitigating Routing Misbehavior in Mobile Ad hoc Networks

Sergio Marti et al. [17], concentrates on thwarting routing misbehaviors that arise from three dimensions: faults, greediness and attacks. They employ mechanisms known as *watchdog* and *pathrater* on DSR to detect the misbehavior of nodes and to rate the routes. The *watchdog* in each node monitors the one-hop neighbor's after transmitting a packet to that neighbor, to confirm whether that neighbor re-transmits the received packet. Each node takes advantage of the *watchdog's* monitored results to rate its one-hop neighbors. Further the nodes exchange their ratings, so that the *pathrater* can rate the paths and choose a path with highest rating for routing. The idea of exchanging ratings genuinely opens door for blackmail attack, where a malicious node can report a benign node to be a misbehaving node due to lack of authenticity.

The *watchdog* cannot differentiate the misbehavior from the ambiguous collisions, receiver collisions, controlled transmission power, collusion, false misbehavior and partial dropping. This creates an uncertainty because of *watchdog's* inability to draw a distinguishable line between the faults and the packet drop attacks. To maintain a balance and offer benefit to uncertainty, the pathrater never rules out a path even if it is suspected to contain packet dropping nodes. As a result, in a roundabout way, not only the *pathrater* favors the packet dropping nodes to continue their misbehavior but also backslides to bring the misbehavior to a halt. The significance of the approach is its initiative to make use of the inherent feature -- promiscuous mode of operation to secure the routing.

#### 5.2.2 Collaborative Trust-Based Secure Routing in Multihop Ad Hoc Networks

In [18], Pissinou et al. attempts to secure routing through the collaborative effort of all nodes. They assume to have pre-distributed trust level among the nodes to achieve the goal. Each ROUTE REQUEST contains a *trust-level* field, which is modified by the receiving intermediate nodes to include the trust level of the node that sends the ROUTE REQUEST. The intermediate node after re-transmitting the ROUTE REQUEST monitors the one-hop neighbors for verification. If any change is found in the one-hop neighbor's re-broadcasted ROUTE REQUEST, the monitoring node generates a warning message similar to the approach in [17]. On successful completion of ROUTE REQUEST phase, the destination chooses the route based on the trust-metric and replies with the ROUTE REPLY, which contains the *next hop* identical to the solution in [16] to avoid the black-hole attack. Whenever duplicates are encountered, the node checks the duplicates consistency, so that it can evaluate the genuineness of its one-hop neighbors. The proposal discourages intermediate nodes from generating route replies.

However, the approach declines to address how the trust is represented, captured and evaluated. It is vulnerable to colluding attacks and fails to handle the route maintenance. The authors fail to address how the trust-

metric is varied depending on the situations and interactions. The pre-distribution of trust is equivalent to the assumption of prior distribution of keys. Though it exploits monitoring technique, it falls short to concentrate selective misbehavior attacks.

#### 5.2.3 CONFIDANT

CONFIDANT protocol [19][20] running in each node has four components - a) *The Monitor*, b) *The Reputation System*, c) *The Path Manager* and d) *The Trust Manager*. Each node monitors its environment through the *Monitor*. Upon detecting a deviating behavior, it invokes the *Reputation System.* The rating in the *Reputation System* gets altered once the action exceeds the threshold limit. Further, if the rating of misbehaving node surpasses intolerable level, then the *Path Manager* is called to take action. The *Path Manager* apart from deleting the misbehaving node in its routes generates an ALARM message to the *Trust Manager,* which can also receive ALARM message externally from the friends or other nodes through the *Monitor* component for trust examination and evaluation. The generated ALARM messages are sent to friends or to the route initiator.

The model doesn't address how to integrate the *Monitor* component with fault tolerance techniques, so that it can mitigate the confusions that may arise in distinguishing the misbehaviors from the genuine faults. The cyclic chain's strength completely relies at two spots: *Reputation System* and *Trust Manager.* In general, the *Reputation System* operates at two stages, one to tick the rating if the misbehaving exceeds the threshold and second to generate a serious action if the rating exceeds the tolerable level. As time proceeds, this two-stage operation indirectly allows the malicious nodes and selfish nodes to conduct *selective misbehaving* – a new form of attack. Moreover the time limit used to refresh false accusations, fault rating and list blow-up, allows the nodes to get away with *selective misbehaving*. Questions on how to decide the threshold factor and the intolerable level are not addressed. The *Trust Manager* fails to handle the issue of how to establish the friends' list. ALARM flooding is another attack that can exploit a node's energy, whereby the incoming ALARM from a non-friend is checked for its trustworthiness and there is no pre-defined limit in committing a node's energy for the *Trust Manager.* Also, the system becomes entangled if two friends report each other to be malicious through ALARM messages. The trust captured is neither dynamic to reflect the malicious and benign behavior of the monitored node, nor displays push-pull behavior to accommodate repenting nodes and exclude compromised nodes.

#### 5.2.4 Discussion

From the detailed study, we observe that not all approaches deploying monitoring technique formalize trust as a computational metric to capture the dynamic events. Some of the approaches which go a step ahead remain entangled during the process of capturing and computing trust. It is very obvious that mere detection-reaction layer void of prevention layer never renders complete security because detection-reaction layer is only an add-on layer to provide more depth in the security design. However, any packet drop event can be classified as intentional or accidental only through the information captured from the dynamic changes in the environment. In order to achieve this faultless classification through detection-reaction layer, it is necessary to consider various perspectives during the process of reputation capture [21]. The knowledge derived from various perspectives enables the detection-reaction layer to spot the selective misbehaviors and the volatility in the medium.

## 6. Need for an Enforcement Layer

Integration of prevention layer with detection-reaction never eliminates packet drop event, though the combination may identify and exclude the selfish or malicious node performing packet drop attack. However, to keep the packet drops at minimum, irrespective of the type of event and to diminish the chance of uncertainty involved in identifying the nodes launching selective packet drops, a radical approach is needed.

Prior to the proposal of *enforcement layer's* incorporation with the other two layers, which is aimed to defend the packet drop event, we considered a series of factors:

- To address the tradition of homogeneous recommendations for heterogeneous resource-constrained environment
- To achieve and secure the basic operation of the protocol rather than to identify and defend list of known attacks
- To involve the participation of individual nodes for the successful functioning of the network

Hence, we propose an enforcement layer which obligates the participants to contribute a significant level of its resources for the essential network services like forwarding others packets, so that it can in turn exist and derive the same services from others. We argue that the imbalances among the nodes are addressed implicitly because a node with a low resource relatively exhausts quickly and until its existence in the network it can contribute its services to the network in order to derive similar services from other nodes. If the low-resource node does not obligate in order to compete with high resource nodes then the combined action of prevention and detection-reaction layer may exclude them. We are currently in the process of designing an enforcement layer that takes the participants transmission queue length and energy as obligation factors. Consequently, we believe it to encourage the basic routing operations, which on other hand may be well supported by the combined action of

prevention layer and detection-reaction layer. The prevention layer assures the protection of the operation and the detection-reaction layer captures the abnormal occurrences.

## 7. Conclusion

In recent years the widespread availability of wireless communications, mobile computing and handheld devices has led to the growth and significance of wireless mobile ad hoc networks. Though there have been many works in the recent years on secure routing protocols, we believe that the "Packet Drop Attack" amongst the nodes is not adequately addressed. In this paper, after analyzing both the class of secure routing protocols (the protocols that deploy cryptographic techniques and the protocols that deploy monitoring techniques); we demonstrated their inability to achieve complete secure routing. From the detailed examination of the packet drop events and the study of secure routing protocols, we proposed an efficient defense-in-depth strategy to secure mobile ad hoc networks through the integration of three layers -- prevention layer (based on cryptographic techniques), detection-reaction layer (based on monitoring technique) and enforcement layer (based on obligations).

## 8. References:


[1] Y.-a. Huang and W. Lee, A Cooperative Intrusion Detection System for Ad Hoc Networks Security. Conference on Computer and Communications, *Proceedings of the 1st ACM workshop on Security of Ad hoc and Sensor Networks*, Fairfax, Virginia, 2003, 135-147.

[2] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks. *10th IEEE International Conference on Network Protocols (ICNP'02),* Paris, France, 2002, 78-89.

[3] Y.-C. Hu and A. Perrig, A Survey of Secure Wireless Ad Hoc Routing, *IEEE Security and Privacy*, *2*(3), 2004, 28 - 39.

[4] N. Milanovic, M. Malek, A. Davidson, and V. Milutinovic., Routing and Security in Mobile Ad Hoc Networks, *IEEE Computer*, *37*(2), 2004, 61- 65.

[5] H. Yang, X. Meng, and S. Lu, Self-Organized Network-Layer Security in Mobile Ad hoc Networks. *International Conference on Mobile Computing and Networking, Atlanta*, GA, USA, 2002, 11-20.

[6] Y.-C. Hu, A. Perrig, and D. B. Johnson, Efficient Security Mechanisms for Routing Protocols. *Network and Distributed System Security Symposium, NDSS '03*, San Diego, USA, 2003, 57-73.

[7] Y.-C. Hu, A. Perrig, and D. B. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. INFOCOM 2003, *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*, 2003, 1976- 1986.

[8] C. E. Perkins, *Ad hoc Networking*, (Boston, Ed.: Addison-Wesley Longman Publishing Co., 2001)

[9] C. E. Perkins, E. M. Royer, S. R. Das, and M. K. Marina, Performance Comparison of two On-demand Routing Protocols for Ad hoc Networks, *IEEE Personal Communications*, *8*(1), Feb 2001, 16 - 28.

[10] M. G. Zapata, Secure Ad hoc On-Demand Distance Vector (SAODV) Routing. *IETF Internet Draft (Work in Progress), draft-guerrero-manet-saodv-00.txt*, 2001.

[11] M. G. Zapata, Secure Ad hoc On-Demand Distance Vector Routing, *ACM SIGMOBILE Mobile Computing and Communications Review*, *6*(3), 2002, 106-107.

[12] M. G. Zapata and N. Asokan, Securing Ad hoc Routing Protocols. *International Conference on Mobile Computing and Networking*, Atlanta, GA, USA, 2002, 1-10.

[13] S. Yi, P. Naldurg, and R. Kravets, Security-Aware Ad hoc Routing for Wireless Networks. *Proceedings of the 2nd ACM international symposium on Mobile ad hoc Networking & Computing*, Long Beach, CA, USA, 2001, 299-302.

[14] S. Yi, P. Naldurg, and R. Kravets, Security-Aware Ad hoc Routing for Wireless Networks. *Technical Report* (UIUCDCS-R-2001-2241), University of Illinois at Urbana-Champaign, USA, August 2001.

[15] S. Yi, P. Naldurg, and R. Kravets, A Security-Aware Routing Protocol for Wireless Ad Hoc Networks. *6th World Multi-Conference on Systemics, Cybernetics and Informatics*, Orlando, Florida, USA, 2002.

[16] H. Deng, W. Li, and D. P. Agrawal, Routing Security in Wireless Ad Hoc Networks, *IEEE Communications Magazine*, *40*(10), Oct 2002, 70- 75.

[17] S. Marti, T. J. Giuli, K. Lai, and M. Baker, Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. *Proceedings of the 6th annual international conference on Mobile Computing and Networking (MOBICOM)*, Boston, Massachusetts, United States, 2000, 255-265.

[18] N. Pissinou, T. Ghosh, and K. Makki, Collaborative Trust-Based Secure Routing in Multihop Ad Hoc Networks. *Third International IFIP-TC6 Networking Conference*, Athens, Greece, 2004, LNCS 3042, 1446-1451.

[19] S. Buchegger and J.-Y. L. Boudec, Performance Analysis of the CONFIDANT Protocol. Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks. *Technical Report* (IC/2002/01), EPFL I&C, Lausanne, Jan 21 2002.

[20] S. Buchegger and J. Y. L. Boudec, Performance analysis of the CONFIDANT protocol. *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing,* Lausanne, Switzerland, Jun 2002, 226-236.

[21] V. Balakrishnan and V. Varadharajan, Designing Secure Wireless Mobile Ad hoc Networks. *Proceedings of the 19th International Conference on advanced information Networking and Applications (AINA 2005),* Taipei, Taiwan, 2005.