International Journal of Research in Engineering, Science and Management
Volume-2, Issue-1, January-2019
www.ijresm.com | ISSN (Online): 2581-5792

An Intrusion Detection Scheme for AODV based Ad Hoc Wireless Network

R. Prasanthi[1], H. Meharban[2]
[1]*Lecturer, Department of Computer Engineering, ADJD Polytechnic College, Nagapattinam, India*
[2]*Lecturer, Department of ECE, ADJD Polytechnic College, Nagapattinam, India*

***Abstract*: Mobile ad Hoc Networks are a new generation of networks offering unrestricted mobility without any underlying infrastructure. Primary applications of Ad Hoc networks are in military, and other security-sensitive operations, where the environment is hostile. Hence security is a critical issue. In MANETs, it is difficult to identify malicious hosts as the topology of the network dynamically changes. A malicious host can easily interrupt a route for which it is one of the forming nodes in the communication path.**

In this paper, an anomaly detection Scheme based on a dynamic learning process that allows the training data to be updated at particular time intervals is proposed. To differentiate an attack state from the normal state, a multidimensional features based on the characteristics of these attacks are defined and utilized.

***Keywords*: mobile ad hoc networks (MANETs), Ad hoc on-demand distance vector (AODV), anomaly detection, dynamic learning, and malicious attacks.**

1. Introduction

A wireless ad-hoc network is a collection of mobile/semi-mobile nodes with no pre-established infrastructure, forming a temporary network. Each of the nodes has a wireless interface and communicates with each other over either radio or infrared. Laptop computers and personal digital assistants that communicate directly with each other are some examples of nodes in an ad-hoc network. Nodes in the ad hoc network are often mobile, but can also consist of stationary nodes, such as access points to the Internet.

Ad-hoc networks are also capable of handling topology changes and malfunctions in nodes. It is fixed through network reconfiguration. For instance, if a node leaves the network and causes link breakages, affected nodes can easily request new routes and the problem will be solved. This will slightly increase the delay, but the network will still be operational.The document starts here. Copy and paste the content in the paragraphs.

The section title also can be copied and paste it, when you need new section and type the section heading as per your requirement.

A. Security goals in ad hoc networking

Because of the sensitive applications of ad hoc network security is a vital factor for MANETs. Securing ad hoc network involves ensuring following attributes:

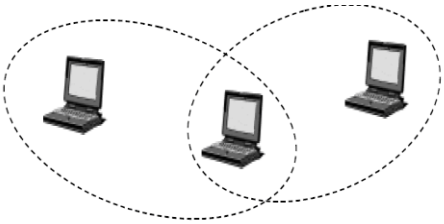

Fig. 1. Simple ad-hoc network with three participating nodes

- Availability implies that the requested service is available even though there is potential problem in the system.
- Confidentiality ensures that classified information is disclosed to only authorized persons.
- Integrity implies that message to be transferred is not altered or tampered on the way. Message modification may be either intentionally or unintentionally. Unintentional modification occurs when there is an impairment of radio propagation.
- Authentication ensures that a communicating entity is communicating with another legitimate entity.
- Non-repudiation ensures that once a message has been sent it cannot deny afterwards. It is particularly useful for detecting compromised node.

B. Security issues in Ad Hoc

- Eavesdropping on the wireless links. Nodes can be hijacked, captured or compromised. Public key & certificate difficult due to no central authority.
- Dynamic topology. Nodes exchange route update information. Attacker can interfere or modify this. DoS possible by flooding w/ routing messages.
- Nodes cooperate to make decisions, an attacker can refuse cooperation and break the algorithm causing breakdown.
- MAC protocols use contention-based method; node competes for TX on channel. Irrelevant of protocol, malicious node can take over the channel and cause DoS.
- MANET has low energy (battery), DoS occurs by

making node send many packets until energy depletes causing disconnection of node.

Because of the wireless medium, lack of central control, cooperation of nodes, limited power and resources, and dynamic topology, security issues are different from wired and even traditional wireless networks.

C. Classification of attacks in Manets

- External attacks are the attacks launched by parties that are not part of the network. External attackers are not necessarily disconnected from the network, though. The targeted network might be a self-contained
  - MAC layer jamming
  - Traffic analysis
- Internal attacks are sourced from inside a particular network. A network with internal attacker nodes is more vulnerable because a malicious node inside a network is already past the basic defence lines of a network, hence the malicious activity is very difficult to detect and curtail.
  - Compromised host sending false routing information
  - Fake authentication and authorization
  - Traffic flooding
- Passive attacks are those attacks in which a malicious node does not actively try to disrupt the network; instead, it sits silently, eavesdropping on communication and data traffic, as well as collection information about the various communicating nodes of a network.
- Active attacks are those in which a node proactively searches for flaws in the network and tries to disrupt the topology of the network by overloading it or breaking existing paths between network nodes.

The typical types of attacks in MANETs include eavesdropping, address spoofing, forged packets, denial of service (DoS), etc. [2]. Secure routing protocols [3]–[4] in which key-based cryptographic technologies [5], [6] are applied have been suggested to meet the increasing demands for MANET security. However, besides the topology issue, these methods cannot protect the network from attacks by a malicious node that has managed to acquire the network key. Therefore, other security methods that can detect attacks from malicious hosts are required. If a well-known attack in the TCP/IP protocol stack is launched in a MANET, then it is possible to protect the network by using conventional security techniques [7]. However, if the attacker maliciously uses the specific routing protocol of the MANET, prevention becomes remarkably difficult [8]. In such a case, it is almost impossible to recognize where and when the malicious node appears. Thus, the attack detection at each node becomes necessary [9].

The techniques for detecting the malicious attacks are usually classified into two categories, namely, Misuse detection and Anomaly detection. In misuse detection, the method of using a signature-based analysis is widely implemented. In this method, the attacks are identified by comparing the input traffic signature with the signatures extracted from the known attacks at the network routers. Anomaly detection is a technique that quantitatively defines the baseline profile of a normal system activity, where any deviation from the baseline is treated as a possible system anomaly. It is rather easy to detect an attack, the traffic signature of which is identifiable by using misuse detection. However, for those attacks, the type or traffic signatures of which are hard to identify by misuse detection, the method is rather inadequate. In such cases, those attacks can only be detected by using anomaly detection methods. In anomaly detection, even when the traffic signature is unknown, if the baseline profile of a network is delineated a priori, then the abnormality can be recognized.

2. Related works

A. Attack detection based on routing procedures

Secure ad hoc routing protocols have been proposed as a technique to enhance the security in MANETs. For example, the secure AODV (SAODV) [11], which uses signed routing messages, is proposed to add security to AODV [10]. A-SAODV [12], [13] is a mild implementation that uses the RSA [14] as an asymmetric cryptographic algorithm and the SHA1 [15] as a hash algorithm.

The survey conducted by Yih-Chun and Perrig [16] overviewed the various secure routing protocols and pointed out their drawbacks and advantages. They also proposed a secure on-demand ad hoc network routing protocol (Ariadne) [17], which prevents the compromised nodes from tampering with the uncompromised routes, and the secure efficient ad hoc distance (SEAD) [18], which is a secure routing protocol, using efficient one-way hashing functions and not using asymmetric cryptographic operations.

In addition, Zhou and Haas proposed a distributed certification authority mechanism in which the authentication uses threshold cryptography [3]. In [19], a MANET is divided into clusters, and a certification authority is appointed to each cluster. In [20], a method called key predistribution (KPD) scheme is applied. In [21], the authenticated routing for ad hoc networks (ARAN) is proposed by using public-key cryptographic mechanisms based on the AODV. These methods can only guard against external attacks. However, the internal attacks mounted by the malicious or compromised hosts may still have a severe impact on the network performance, as well as on the connectivity among the nodes in the targeted MANET.

Deng et al. [22] proposed an approach that requires the intermediate nodes to send a route reply (RREP) packet with the next hop information. When a source node receives the RREP packet from an intermediate node, it sends a “Further Request” packet to the next hop to verify that it has a route to the intermediate node and a route to the destination. As a

response to this request, the intermediate node will send another RREP packet. When the next hop receives a "Further Request" packet, it sends a "Further Reply" packet that includes the verified result to the source node. Based on the information in the "Further Reply" packet, the source node judges the validity of the route. Again, the method in [23] requires the intermediate node to send the route confirmation request (CREQ) to the next hop node toward the destination, and then, the next hop node receives the CREQ and looks into its cache for a route to the destination. If it has such a route to the destination, then it sends a route confirmation reply (CREP) message to the source node with its route information. The source judges whether the path in RREP is valid by comparing the information with CREP. In these methods, the routing protocol has to be modified. These modifications may increase the routing overheads, which results in the performance degradation of the bandwidth-limited.

B. Attack detection based on network monitoring

Network monitoring can be used to detect attacks from inside MANETs. Kachirski and Guha [24] proposed a method that detects attacks by employing distributed mobile agents. Network monitoring nodes are selected to be able to collect all the packets within a cluster, and the decision agents in the nodes are used to detect and classify the security violations. This method will consume a large amount of energy.

Vigna et al. [25] detect attacks by placing AODV-based State Transition Analysis Technique (AODVSTAT) sensors within the network and by either observing solely contiguous nodes or trading information with other sensors. However, it is necessary to deploy a large number of AODVSTAT sensors on the nodes for detecting a varied range of attacks. In addition, a large number of UPDATE messages may cause an overwhelming congestion in the network.

Tseng et al. [26] introduced a method that places a network monitor (NM) inside the network. In this method, the NM constantly monitors the packet flow in the network within a certain range to detect any attacks. However, placing effective detectors, i.e., mobile agents, sensors, or NMs, is considered to be difficult when the MANET topology dynamically changes. One solution to this problem is to observe the packet flow on each node and to detect any potential attack.

Huang et al. [27] proposed a method in which the packet flow is observed at each node. They suggested an anomaly detection mechanism with interrelation between 141 features which are traffic and topology related. Moreover, in [28], they constructed an extended finite-state automaton (EFSA) according to the specification of the AODV routing protocol, envisioned normal condition modeling, and detected attacks with both specification-based and anomaly-based detection schemes. In specification-based detection, the attacks were detected as deviant packets from the conditions defined by EFSA. In addition, in anomaly detection, the normal conditions are defined as the baseline with which the condition of EFSA and also the amounts of transition statistics are compared. The deviations from those conditions are then used to detect the potential attacks. For determining the baseline profiles, in both methods, the training data are extracted beforehand from the same network environment where the test data are applied.

The MANET topology can easily be changed, so the differences in network states grow larger with time. Furthermore, these methods cannot be applied to a network where the learning phase has been conducted in another network.

C. Anomaly detection

Sun et al. [29] proposed an anomaly detection method in which mobility is considered. This method computes the recent link change rate (LCRrecent) and can select the training data, the link change rates of which have the smallest Euclidean distance to LCRrecent. However, the change of network states can be caused not only by mobility; it may also occur due to the sudden participation and disappearance of nodes in a MANET. When the nodes in the current MANET differ from those in the training data, the defined baseline profile cannot express the current network state. As a result, these methods are rendered inadequate and considered difficult in a MANET environment.

To solve this problem, a normal state needs to be defined by using the data reflecting the trend of the current situation, and this leads to the idea of updating the learning process within a time interval. By doing so, the attack detection can adaptively be conducted even in a changing network scenario.

3. AODV protocol

A. Overview of AODV Protocol

The above section says how to prepare a subsection. Just copy and paste the subsection, whenever you need it. The numbers will be automatically changes when you add new subsection. Once you paste it, change the subsection heading as per your requirement.

The AODV [16] is a reactive routing protocol in which the network generates routes at the start of communication. Each node has its own sequence number, and this number increases whenever a link changes. According to its sequence number, each node judges whether the channel information is recent.

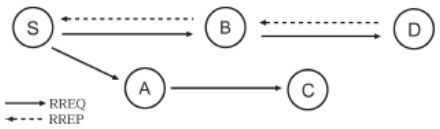

Fig. 2. Route-discovery process on AODV

In Fig. 2. Node S attempts to establish a connection to destination D. First, the source node S refers to the route map at the start of communication. In the case where there is no route to destination node D, it sends a route request (RREQ) message by using broadcasting. The RREQ ID is increased by one every time node S sends an RREQ message. Nodes A and B have received the RREQ message, generate and renew the route to its previous hop. They also evaluate if this is a repeated RREQ

message and accordingly discard it. If A and B have a valid route to the destination D, then they send an RREP message to node S. In the case where the node has no valid route, they send an RREQ message using broadcasting. The exchange of route information will be repeated until an RREQ message reaches node D. When node D receives the RREQ, it sends an RREP message to node S. When node S receives the RREP message, a route is established. In case of multiple RREPs received, a node selects an RREP message, the Destination Sequence number (Dst_Seq) of which is the largest among all the previously received RREPs. However, if the Dst_Seqs were the same, then it will select the RREP message whose hop count is the smallest.

In Fig. 2, when node B detects a disconnection of route, it generates route error (RERR) messages and puts the invalidated address of node D into its list and then sends RERR to node A. When node A receives the RERR message, it refers to its route map and the current list of RERR messages. If there was a route to the destination for node D included in its map, and the next hop in the routing table is a neighboring node B, it invalidates the route and sends an RERR message to node S. This way, the RERR message can finally be sent to the source node S.

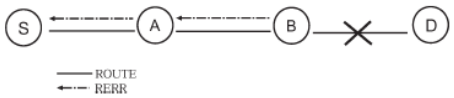

Fig. 3. Transferring RERR messages on AODV

B. *Attacks on AODV*

1) *Authentication and non-repudiation attacks*

Authentication allows a node to verify the identity of a peer node with which it is communicating. Non-repudiation is the ability to prove that a sender sent a message. Most ad hoc routing protocols use either MAC or IP addresses to uniquely identify hosts in the network. Therefore, spoofing one of these two addresses is the simplest method to attack the security goals of authentication and non-repudiation

2) *Availability attacks*

Availability guarantees that network services (e.g., bandwidth and connectivity) are accessible to authorized entities in a timely manner. The following sections present a variety of denial-of-service attacks, which are used to reduce or completely deny the availability of network services.

- Dropping of Packets.
- Fabrication Attacks.
- Resource Depletion Attacks.
- Selective Existence Attacks.

3) *Integrity attacks*

Integrity guarantees that a message is not altered on its path to the destination. In the following, a variety of integrity attacks are discussed.

- False Message Propagation Attacks.
- Misrouting Attacks.
- Man-in-the-Middle Attacks.

4) *Confidentiality and privacy attacks*

Privacy guarantees non-disclosure of personal information stored at a node to any other node in the network. Confidentiality ensures that certain information is disclosed only to authorize entities.

- Location Disclosure Attacks.
- Content Disclosure Attacks.

4. Proposed approach

In the proposed modified anomaly detection scheme, each node builds a profile for every one of its neighbours. The profile includes all features listed below. A node can use a profile by keeping it to monitor its neighbour node's behaviour.

In this section, we first introduce the features that are essential for anomaly detection scheme, and then delineate the module of the detection scheme.

Table 1
List of features

S. No.	Description of feature
	I. Path Finding Features
1.	Number of received RREQ messages.
2.	Number of forwarded RREQ messages
3.	Number of outbound RREQ messages
4.	Number of outbound RREP messages
5.	Number of received RREP messages
	II. Path Abnormality Features
1.	Number of received RERR messages
2.	number of outbound RERR messages
3.	Number of dropped RREQ messages
4.	Number of dropped RREP messages

A. *Baseline profile definition*

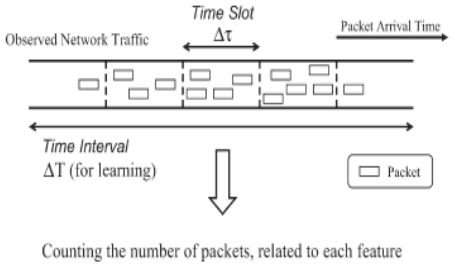

Fig. 4. Feature definition

Each node builds a profile for every one of its neighbours. A baseline profile is usually used to verify the identity and the topology of the network, thus preventing any malicious host from joining the network. Since the topology of a MANET dynamically changes, the use of a static baseline profile is not efficient.

In our baseline profile method the training data for every timeslots are stored i.e. the number of packets that are transmitted or received by a particular node in a network are stored. The profile includes all features listed in Table 1.

B. *Route discovery (neighbor detection)*

AODV is the routing protocol which is used for the route discovery in the network. Consider node S attempts to establish a connection to destination D. First, the source node S refers to

the route map at the start of communication. In the case where there is no route to destination node D, it sends a route request (RREQ) message by using broadcasting. The RREQ ID is increased by one every time node S sends an RREQ message. Nodes A and B are intermediate nodes between the source S and destination D, which have received the RREQ message, generate and renew the route to its previous hop. They also evaluate if this is a repeated RREQ message and accordingly discard it. If A and B have a valid route to the destination D, then they send an RREP message to node S. In the case where the node has no valid route, they send an RREQ message using broadcasting. The exchange of route information will be repeated until an RREQ message reaches node D. When node D receives the RREQ, it sends an RREP message to node S. When node S receives the RREP message, a route is established. In case of multiple RREPs received, a node selects an RREP message, the Destination Sequence number (Dst_Seq) of which is the largest among all the previously received RREPs. However, if the Dst_Seqs were the same, then it will select the RREP message whose hop count is the smallest.

When node B detects a disconnection of route, it generates route error (RERR) messages and puts the invalidated address of node D into its list and then sends RERR to node A. When node A receives the RERR message, it refers to its route map and the current list of RERR messages. If there was a route to the destination for node D included in its map, and the next hop in the routing table is a neighboring node B, it invalidates the route and sends an RERR message to node S. This way, the RERR message can finally be sent to the source node S.

C. Dynamic anomaly detection

Since the network topology easily changes in MANET, the current state may not appropriately be expressed over time. Therefore, dynamically updating the training data sets to reflect the changing situation of MANET, and a learning method that can follow these changes is indispensable.

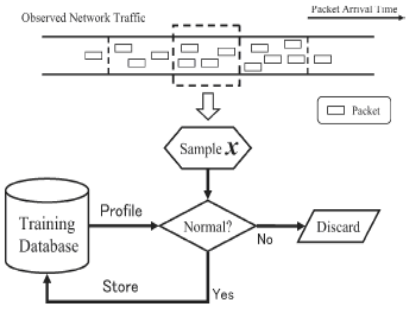

Fig. 5. Flow chart of the learning and evaluation method

Let T0 be the current time interval, and let T1 be the first time interval. By using the data collected in T1 is used in the following time interval T0 for anomaly detection. If the state in T0 is judged as normal, then the corresponding data set will be used as the training data set. Otherwise, it will be treated as the data including attack, and it will consequently be discarded. This way, we keep on learning the normal states of the network. When updating the database, it is possible to use the most recent data set. However, since the most recent data set is easily affected by the sudden change in the network, it is necessary to take the time series model into consideration to keep the database from being too sensitive to the changes in the network topology.

D. Intimation to sender

The information of the intruder is sent to the sender.

5. Principle component analysis

The PCA (Principle Component Analysis) explores the correlation between the number of received, dropped and forwarded control packets in every node with normal network condition and the network with the attacks. The training data are recorded once for each time slot.

This work proposes a computationally efficient method that exploits the structure of the principal components of a feature set to find a subset of the original feature vector. The chosen subset of features is shown empirically to maintain some of the optimal properties of PCA. It is a classic technique in statistical data analysis, feature extraction and data compression. Goal is to find a smaller set of variables in a set of multivariate measurements with less redundancy.

The starting point for PCA is a random vector x with n elements. There are available samples x(1) . . . x(T) from this random vector. No explicit assumptions on the probability density of the vectors are made in PCA, as long as the first and the second-order statistics are known or can be estimated from the sample. No generative model is assumed for vector x. The elements of x are measurements like values of a signal at different time instants [16]. In the PCA transform, the vector x is first centered by subtracting its mean:

$x = x - E\{x\}$

In practice, the mean is estimated from the available sample x(1) . . . x(T). The matrix X is a n × n covariance matrix of x.

$C_x = E\{xx^T\}$

It is well known from basic linear algebra that the solution to the PCA problem is given in terms of the unit-length eigenvectors $e_1, e_2, \ldots, e_n$ of the matrix C_x. The ordering of the eigenvectors is such that the corresponding Eigen values $d_1, \ldots, d_n$ satisfy $d_1 >= d2 >= , \ldots ,>= d_n$.

Thus the first principal component of x is

$y_1 = e_1^T x$.

6. Simulation environment

The experiments were carried out by using ns-2. We assume that the simulation network being used is in a place where various events in a MANET can occur. 50-node network with a network topology of 1000 m × 1000 m. The traffic loads were constant bit rate flows with a data packet size of 512 B. The load was varied by using 40 flows (at four packets per second). The 802.11 Media Access Control (MAC) layer was used with

a transmission range of 250 m, and it was set for a 2-Mb/s throughput. As for the moving pattern for each node, we use a random waypoint (RWP) model in which each node randomly selects the destinations in the designated simulation area with random speeds. Here, the node velocity was set between 0 and 5 m/s. The pause time was set to 10, 50, 100, 200, and 500 s, respectively.

7. Conclusion

This approach can reduce the overhead of monitoring the networks. A normal state of operation is separated from the attack state by detecting deviation of certain feature values and selected parameters. A dynamic anomaly detection system for MANETs has been proposed for enhancing the security in MANETs.

Future works will be focused to develop simulations to analyze the performance of the proposed solution and analysis of additional types of attacks.

References

[1] Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour, Yoshiaki Nemoto and Nei Kato, "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks", IEEE Transactions On Vehicular Technology, Vol. 58, No. 5, June 2009 2471,
[2] P. Argyroudis and D. O'Mahony, "Secure routing for mobile ad hoc networks," Commun. Surveys Tuts., vol. 7, no. 3, pp. 2–21, Third Quarter, 2005.
[3] L. Zhou and Z. Haas, "Securing ad hoc networks," IEEE Netw., vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.
[4] P. Papadimitratos and Z. Haas, "Secure data transmission in mobile ad hoc networks," in Proc. ACM Workshop WiSE, Sep. 2003, pp. 41–50.
[5] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.
[6] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, Handbook of Applied Cryptography. Boca Raton, FL: CRC, 1996.
[7] J. Edney and W. Arbaugh, Real 802.11 Security: Wi-Fi Protected Access 802.11i. Upper Saddle River, NJ: Pearson, 2004.
[8] C.-K. Toh, Ad Hoc Mobile Wireless Networks-Protocol and Systems. Upper Saddle River, NJ: Pearson, 2002.
[9] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," IEEE Wireless Commun., vol. 11, no. 1, pp. 48–60, Feb. 2004.
[10] C. Perkins, E. Belding-Royer, and S. Das, Ad hoc On-Demand Distance Vector (AODV) Routing, Jul. 2003. IETF RFC 3561 (Experimental).
[11] M. Zapata, Secure ad hoc on-demand distance vector (SAODV) routing, Sep. 2006. IETF Internet Draft, draft-guerrero-manet-saodv-06.txt.
[12] A-SAODV Homepage. [Online]. Available: http://saodv.cefriel.it/
[13] D. Cerri and A. Ghioni, "Securing AODV: the A-SAODV secure routing prototype," IEEE Commun. Mag., vol. 46, no. 2, pp. 120–125, Feb. 2008.
[14] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.
[15] D. Eastlake, III and P. Jones, US Secure Hash Algorithm 1 (SHA1), Sep. 2001. IETF RFC 3174 (Informational).
[16] H. Yih-Chun and A. Perrig, "A survey of secure wireless ad hoc routing," IEEE Security Privacy, vol. 2, no. 3, pp. 28–39, May/Jun. 2004.
[17] H. Yih-Chun, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," Wirel. Netw., vol. 11, no. 1/2, pp. 21–38, Jan. 2005.
[18] H. Yih-Chun, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," Ad Hoc Netw., vol. 1, no. 1, pp. 175–192, Jul. 2003.
[19] A-SAODV Homepage. [Online]. Available: http://saodv.cefriel.it/
[20] M. Bechler, H.-J. Hof, D. Kraft, F. Pahlke, and L. Wolf, "A clusterbased security architecture for ad hoc networks," in Proc. 23rd Annu. Joint Conf. IEEE Comput. Commun. Soc. INFOCOM, Mar. 2004, pp. 2393–2403.
[21] M. Ramkumar and N. Memon, "An efficient key predistribution scheme for ad hoc network security," IEEE J. Sel. Areas Commun., vol. 23, no. 3, pp. 611–621, Mar. 2005.
[22] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "Authenticated routing for ad hoc networks," IEEE J. Sel. Areas Commun., vol. 23, no. 3, pp. 598–610, Mar. 2005.
[23] H. Deng, W. Li, and D. Agrawal, "Routing security in ad hoc networks," IEEE Commun. Mag., vol. 40, no. 10, pp. 70–75, Oct. 2002.
[24] S. Lee, B. Han, and M. Shin, "Robust routing in wireless ad hoc networks," in Proc. 31st ICPP Workshops, Aug. 2002, pp. 73–78.
[25] O. Kachirski and R. Guha, "Effective intrusion detection using multiple sensors in wireless ad hoc networks," in Proc. 36th Annu. HICSS, Jan. 2003, pp. 57–64.
[26] G. Vigna, S. Gwalani, K. Srinivasan, E. Belding-Royer, and R. Kemmerer, "An intrusion detection tool for AODV-based ad hoc wireless networks," in Proc. 20th ACSAC, Dec. 2004, pp. 16–27.
[27] C. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A specification-based intrusion detection system for AODV," in Proc. 1st ACM Workshop SASN, Oct. 2003, pp. 125–134.
[28] Y. Huang,W. Fan,W. Lee, and P. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies," in Proc. 23rd ICDCS, May 2003, pp. 478–487.
[29] Y. Huang and W. Lee, "Attack analysis and detection for ad hoc routing protocols," in Proc. 7th Int. Symp. RAID, Sep. 2004, pp. 125–145.