International Journal of Computer Science and Network (IJCSN)
Volume 1, Issue 3, June 2012   www.ijcsn.org   ISSN 2277-5420

Detecting Sinking Behavior at MAC and Network Layer Using SVM in Wireless Ad hoc Networks

[1]K.Kiruthika Devi, [2]M.Ravichandran

**[1] INFORMATION TECHNOLOGY, SRI VENKATESHWARA COLLEGE OF ENGINEERING
CHENNAI, TAMIL NADU ,INDIA**

**[2]COMPUTER SCIENCE, SRI VENKATESHWARA COLLEGE OF ENGINEERING
CHENNAI, TAMIL NADU,INDIA**

Abstract

Wireless Ad hoc networks present more security problems than the conventional wired and wireless networks because of the nature of dynamically changing and a fully decentralized topology. As the Ad hoc network lacks infrastructure the nodes have to cooperate for services like routing and data forwarding. This paper proposes a Autonomous Intrusion Detection System using SVM. The feature set are constructed from MAC layer and Network layer to profile the normal behavior and malicious behavior of wireless node. The training data consist of both normal and abnormal behavioral patterns. Hence the proposed system identifies both anomaly and Misbehavior of nodes in the network. Simulation is done under various network conditions and malicious node behavior. The features identified are obtained by analyzing the data from the trace log.These feature values obtained are created by simulating wireless node behavior and used by SVM to detect intrusions.

Keywords: Intrusion Detection,Wireless Ad hoc Networks, Sinking , Multi layer attacks, Network security.

I. INTRODUCTION

A Wireless Ad hoc network is a collection of wireless mobile hosts network with autonomous nodes. Vulnerability of wireless networks keeps with technology. In a wireless network, one cannot make the assumption that wireless users are trusted. Also,the network is distributed, decentralized, and dynamic due to mobility. As the Ad hoc network lacks infrastructure and centralized nodes, the nodes have to cooperate for services like routing and data forwarding. Wireless networks are more vulnerable due to the nature of mobility and decentralized topology .Hence there is a need of security measures for wireless networks. Intrusion prevention measures such as authentication and encryption are not guaranteed to work all the time, which brings out the need to complement them with efficient intrusion detection and response. If an intrusion is detected quickly enough the intruder can be ejected before any damage is done or any data is compromised. An effective IDS can not only serve as a deterrent acting to prevent intrusions but also provide information about intrusions to strengthen intrusion prevention measures.

Section II describes vulnerabilities of wireless network. Section III describes related work. Section IV describes feature of interest. Section V describes wireless intrusion detection architecture. Section VI describes experiment results and performance evaluation.

II. VULERABILITIES OF WIRELESS NETWORK

In an Ad hoc network, there are four kinds of routing attacks which are spoofing, fabrication,sinking and flushing. This paper is worked taking Sinking behavior of the node. Sinking behavior is a malicious behavior of nodes where nodes do not cooperate in the routing and forwarding operations of the network. Nodes exhibiting sinking behavior maliciously drop data or routing messages. Nodes exhibiting this behavior does this to selfishly evade for resource conservation or to disrupt the network by dropping critical packets. The proposed IDS consists of three entities and their characteristics to define the threat model.The entities are the network,the attack, and the attacker. .Characteristics of the network include factors that help to hide the malicious behavior. These characteristics of the network cause nodes to benignly drop packets. This kind of dropping behavior due to the network conditions resembles the behavior of malicious sinking. Therefore, the goal of the IDS is to distinguish packet dropping induced by network conditions and from those caused by malicious sinking. Possible factors which can induce benign dropping include the following:

. mobility of nodes,
. network/traffic density,
. traffic type ,
. channel and fading conditions.

An active route can become broken due to mobility. Here the dropping of the packets becomes inevitable, as reestablishing a new route takes some time. The characteristics of the attacker or the attack also challenge the IDS. The characteristics include the following:

. duration of attack,
. drop ratio (i.e., the percentage of data dropped).

If the attack is sporadic, the detection efficiency reduces. A node’s sporadic attack behavior has high resemblance with benign dropping due to the network conditions. Similarly, the sinker can selectively drop critical data/ routing packets and forward some percentage of inbound traffic benignly. This kind of intelligent strategy by the attacker will render detection hard. The proposed IDS model is studied with varying conditions of the above factors.

III.RELATED WORK

Most of current works on IDS for wireless networks employ either distributed and cooperative architecture or distributed and hierarchical architecture. Zhang [6] in their work proposed a cooperative distributed IDS architecture, which became the standard for IDS architecture in Ad Hoc networks.In their model, a global and local detection system is used.Global IDS of the model aids the local IDS (LIDS) of individual nodes in deciding over an intrusion. In return LIDS provides any newly acquired knowledge to the global IDS which is stored in a centralized global knowledge base. Therefore, whenever a node’s LIDS faces uncertainty in deciding over an intrusion it will seek help from the global deciding over an intrusion. The detection engine used an SVM light algorithm for classifying normal and malicious routing behaviors.

Table-driven routing protocols like OLSR are inherently poor in security and more vulnerable to threats as detailed in [12]. In the literature, a few cross-layer approaches for IDS have been proposed. Most of them use layers from MAC or network statistics. In [10], the authors proposed a cross-layer-based IDS architecture, which has an intrusion detection module in every layer. The output from the intrusion detection modules is combined and decision is made collectively. The detection algorithm used a simple but effective rule based system. Though the results were good, IDS in every layer increases the overhead. Furthermore, the system is non adaptable as they do not learn new attacks.

Similarly, Liu et al. [9] proposed a novel distributed cross-layer IDS for Ad Hoc networks. Two layers Network and MAC layers statistics are used for detection. To reduce the feature set a correlated feature set is used. Though the results were promising the experiments were not comprehensive. For example their experiments used a mobility model using maximum mobility of 5 m/s. This is relatively simple environment for intrusion detection and results from these simulations are practically unreliable.

SVM is becoming more popular as a learning technique in numerous domains. In [3], the authors proposed an SVM-based approach for distributed intrusion detection in Ad Hoc networks. Similar to Zhang et al.’s work, the IDS consists of global IDS which aids local IDSs that are present locally in the nodes. However instead of a single global IDS the architecture uses cluster heads that form a hierarchical IDS. This structure increases the reliability of global IDS and knowledge sharing. The choice of using SVM over other machine learning techniques was not justified.

IV.FEATURE OF INTEREST

In wireless networks MAC layer manages and maintains communication between mobile nodes by coordinating access to a shared radio channel and utilizing protocols that enhance communications over a wireless medium. The proactive mechanisms are employed in wireless networks before any data communication. These mechanisms cannot give prefect prevention. This work concentrates on reactive mechanism which detects intrusion or anomaly behavior in wireless networks. To characterize wireless node behavior in wireless network feature set are extracted from MAC layer and network layer.

Features Identified at MAC Layer	Features Identified at Network Layer
MAC Sent Packets	Router Sent Packets

MAC Received Packets	Router Recieved Packets
MAC Dropped Packets	Router Dropped Packets
No of RTS Packet	End to End Delay
No of CTS Packet	Throughput
No of Collisions	Packet Delivery Ratio
Total Dropped Packets	

Table 1: Wireless Feature Set

Total Dropped packets is computed as:
Total Dropped packets = MAC dropped packets + Router dropped packets. (1)

End to End Delay = end time – start time(based on the sequence number of packets) (2)

Packet Delivery Ratio = MAC Received packets/MAC sent Packets. (3)

Throughput = (MAC sent packets *512*8)/end time (4)

V. WIRELESS INTRUSION DETECTION ARCHITECTURE

The goal of intrusion detection is seemingly simple: to detect intrusions and also to identify unauthorized use, misuse and abuse of wireless nodes by both internal attackers and external penetrations. In other words, Intrusion detection is a process of identifying and responding to malicious activity targeted at computing and network resources. A network intrusion is a sequence of activities by a malicious individual that results in unauthorized security threats to a target network. Generally, Intrusion detection is classified as 1.Profile based intrusion detection 2.Signature based detection. Designing an IDS in wireless networks is tougher challenge due to vulnerabilities and lack of physical infrastructure. Without centralized audit point such as routers and gateways, an IDS for wireless networks is limited to using only the current traffic coming in and out of the node. This paper describes wireless intrusion detection architecture to monitor and detect the malicious activity of wireless node. The entire architecture consists of wireless traffic capturing module, Data Collection module, Profile Module,Detection module and Prediction module. The first step is to collect the wireless feature set using NS2 under different network conditions and malicious behaviors

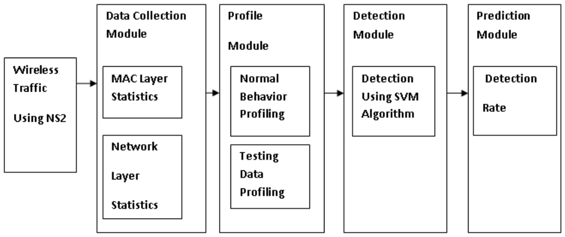


Figure 1.Wireless Intrusion Detection Architecture using SVM

The trace files are generated for scenarios of nodes under different mobility. The data sets are obtained by using awk scripts for each and every scenarios iterated under different simulation times. A script for one of the scenario is given below.

```
BEGIN
{
 seqno = -1;
 droppedPackets = 0;
 receivedPackets = 0;
 sentPkts = 0;
 MACsentPkts = 0;
 MACrecvedPkts = 0;
 routesentPkts = 0;
 routerecvedPkts = 0;
 e2edelay =0;
 macrtsdelay =0;
 macctsdelay =0;
 macackdelay=0;
 RouterdroppedPackets =0;
 MACdroppedpkts=0;
 rtspkt = 0;
 ctspkt =0;
 ackpkt =0;
 col = 0;
 count = 0;
 endtime=0;
}
 {
  if( $1 == "s" && $4 == "MAC"  )
 {
   MACsentPkts++;
  }
 else if($4 == "RTR" && $1 == "r" )
  {
   seqno = $6;
   MACrecvedPkts++
    }
  else if($4 == "AGT" && $1 == "s" )
   {
    seqno = $6;
    routesentPkts++;
    }
   else if($4 == "AGT" && $1 == "r" )
   {
     seqno = $6;
     routerecvedPkts++;
    }
    else if ( $4 == "RTR"  && $1 == "D")
   {
     RouterdroppedPackets++;
    }
    else if ( $4 == "MAC"  && $1 == "D")
     {
      MACdroppedpkts++;
     }
    else if ( $7 == "RTS"  && $1 == "r" || $1 == "s" )
     {
      rtspkt++;
      }
     else if ( $7 == "CTS"  && $1 == "r" || $1 == "s")
     {
      ctspkt++;
      }
     else if ( $7 == "ACK"  && $1 == "r" || $1 == "s")
      {
        ackpkt++;
       }
      else if ($1 == "D"  )
      {
       col++;
       }
      if($4 == "MAC" && $1 == "s")
      {
       start_time[$6] = $2;
}
else if(($7 == "AODV") && ($1 == "r"))
{
  end_time[$6] = $2;
  e2edelay = end_time[$6] - start_time[$6];
  endtime =end_time[$6];
 }
 }

END
{
    for(i=0; i<=seqno; i++)
     {
       delay[i] = end_time[i] - start_time[i];
       count++;
      }
     for(i=0; i<=seqno; i++)
    {
       n_to_n_delay = n_to_n_delay + delay[i];
     }

print  MACsentPkts "\t" MACrecvedPkts "\t"
routesentPkts"\t " routerecvedPkts"\t " MACdroppedpkts
"\t" RouterdroppedPackets "\t "
RouterdroppedPackets+MACdroppedpkts "\t
",e2edelay*1000"ms" "\t" MACrecvedPkts/MACsentPkts
"\t "(MACsentPkts*512*8/endtime)/1000"kbps" "\t "
rtspkt "\t" ctspkt "\t " ackpkt "\t " col;
```

The second module is extracting the features from MAC layer and Network layers.The MAC layer parameters and network layer parameters are identified to profile normal and abnormal behaviors and the parameters are listed in section II as features of interest.

The third module is profiling normal and abnormal behaviors .The normal behaviors represent the nodes under different mobility and traffic density.The data sets are obtained by simulating the wireless scenario for nodes with mobility of 5m/sec,10m/sec,15m/sec,20m/sec, 25m/sec,30m/sec, 35m/sec,40m/sec. The traffic is the transmission of packet by nodes.That is varied by 40%,70%,90%.The sinking behavior is simulated by nodes of varying dropping ratios as 30%,50%,70%,90%.The datasets are obtained for all these by iterating under different simulation times to profile normal and abnormal behaviors.

The fourth module is training and validating the datasets using SVM.In SVM there are two modules .The modules are training and prediction.The datasets are trained and the test set is used to validate the trained datasets.The prediction module determines how accurate it validates the test data with the trained data.

The fifth module is the detection rate.The detection rate is predicted with the set of data sets for nodes under different mobility and traffic density and packet drop.

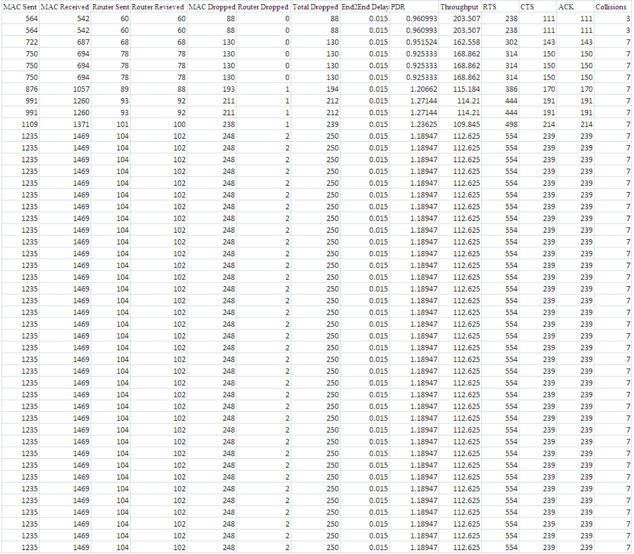
VI. PERFORMANCE OF WIRELESS INTRUSION DETECTOR

A. Results and Analysis

To validate the efficiency of the proposed IDS model, different sinking scenarios over varying network conditions are studied. In mobility scenarios, the node mobility is varied and how mobility affects the detection rate is studied. Similarly drop ratio is experimented and the effect of these conditions over detection efficiency is studied. Simulations are based on a 700 by 200 meters flat space, scattered with 20 mobile nodes. The nodes move from a random starting point to a random destination with a speed that is randomly chosen (the speed is uniformly distributed between 0 to maximum speed). Maximum movement speed of each node is 40*m/s*. Once the destination is reached, another random destination is targeted after a pause time. We choose the pause time to be 0 seconds, which corresponds to a continuous motion of mobile nodes. The simulation time is 900s.Experimention was done with sending rates of 4 packets per second, network containing randomly generated 15 CBR sources and packet sizes of 512 bytes. The traffic files are generated such that the source and destination pairs are randomly spread over the entire network.

The scenarios are created for varying node mobility, packet drop ratio,traffic density.The data sets are obtained from the trace files created using awk scripts.

The feature values are obtained using the awk scripts and the data sets are obtained for nodes with varying mobility conditions,varying traffic density,varying packet drop ratios.One of the sample data set for nodes with mobility of 5m/sec .is given in the table below.



MAC Sent	MAC Received	Router Sent	Router Revieved	MAC Dropped	Router Dropped	Total Dropped	End2End Delay	PDR	Throughput	RTS	CTS	ACK	Collisions
564	542	60	60	88	0	88	0.015	0.960993	203.507	238	111	111	3
564	542	60	60	88	0	88	0.015	0.960993	203.507	238	111	111	3
722	687	68	68	130	0	130	0.015	0.951524	162.558	302	143	143	7
750	694	78	78	130	0	130	0.015	0.925333	168.862	314	150	150	7
750	694	78	78	130	0	130	0.015	0.925333	168.862	314	150	150	7
750	694	78	78	130	0	130	0.015	0.925333	168.862	314	150	150	7
876	1057	89	88	193	1	194	0.015	1.20662	115.184	386	170	170	7
991	1260	93	92	211	1	212	0.015	1.27144	114.21	444	191	191	7
991	1260	93	92	211	1	212	0.015	1.27144	114.21	444	191	191	7
1109	1371	101	100	238	1	239	0.015	1.23625	109.845	498	214	214	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7
1235	1469	104	102	248	2	250	0.015	1.18947	112.625	554	239	239	7

Table 2: Data set for node mobility of 5m/sec

B.Intrusion Detection

The detection rate is used as the performance metrics to evaluate our proposed intrusion detection system. The following Table shows the Detection Accuracy with nodes of varying the range of node mobility, Traffic density and Dropping Ratio.

Table 3: Detection Accuracy for SVM based Model (SVMDM) for Node Mobility

Node Mobility (ms)	Detection Efficiency(%)
5	95
15	96
20	96
25	91
30	95
35	94
40	94

Table 4: Detection Accuracy for SVM based Model (SVMDM) for Traffic Density

Traffic Density(%)	Detection Efficiency(%)
40%	95
70%	96
90%	96

Table 5: Detection Accuracy for SVM based Model (SVMDM) for Dropping Ratio

Dropping Ratio(%)	Detection Efficiency(%)
30% dropping	95
50% dropping	96
70% dropping	96
90% dropping	91

The following Figure shows the detection Accuracy with nodes of varying the range of node mobility, Traffic density and Dropping Ratio.

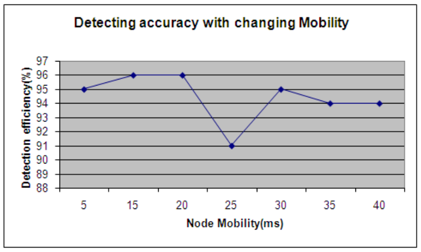


Figure: 2 Detecting accuracy with changing mobility

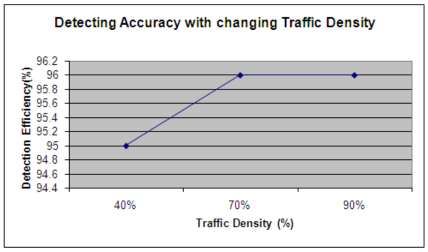


Figure: 3 Detecting accuracy with changing traffic density

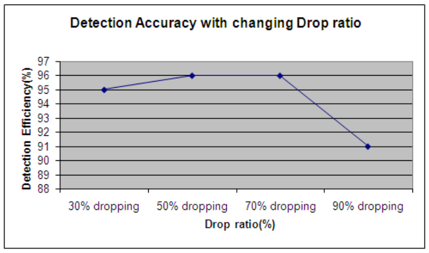


Figure 4. Detection accuracy with changing drop ratio

VII CONCLUSION

In this work Intrusion Detection System for detecting sinking behavior using SVM is proposed and its efficiency is analyzed by simulating under different network conditions and sinking behaviors.In this work features were extracted from multiple layers . The feature set are constructed from MAC layer and Network layer to profile the normal behavior and malicious behavior of wireless node.Simulations are carried out under varying different network conditions and sinking behavior and are analyzed. The proposed work was carried out for sinking behavior .Hence the future work will include distributed architecture for detecting all type of routing attacks using SVM.

References

[1] John Felix Charles Joseph, Bu-Sung Lee,Amitabha Das, and Boon-Chong Seet, ,"Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 2, MARCH-APRIL 2011.

[2] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection in Wireless Ad Hoc Networks," IEEE Wireless Comm., vol. 11, no. 1,pp. 48-60, Feb. 2004.

[3] H. Deng, Q.-A. Zeng, and D.P. Agrawal, "SVM-Based Intrusion Detection System for Wireless Ad Hoc Networks," Proc. IEEE 58thVehicular Technology Conf. 2003 (VTC '03-Fall), vol. 3, pp. 2147-2151, 2003.

[4] Y. Liu, Y. Li, and H. Man, "MAC Layer Anomaly Detection in AdHoc Networks," Proc. Sixth Ann. IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005.

[5] K. Nadkarni and A. Mishra, "Intrusion Detection in MANETS—the Second Wall of Defense," Proc. 29th Ann. Conf. IEEE Industrial Electronics Soc. (IECON '03), 2003.

[6] G.Y.Zhang, W.Lee and Y.A Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", ACM J.Wireless Networks, vol 9,no.5, September 2003 pp.545-56.

[7] J.F.C. Joseph et al., "CRADS: Integrated Cross Layer Approach for Detecting Routing Attacks in

MANETs," Proc. Wireless Networking and Comm. Conf. (WCNC), 2008.

[8] C.-C. Chang and C.-J. Lin, LIBSVM: A Library for Support Vector Machines, 2001.

[9] Y. Liu, Y. Li, and H. Man, "Short Paper: A Distributed Cross-Layer Intrusion Detection System for Ad Hoc Networks," Proc. First Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks 2005 (SecureComm '05), 2005.

[10] G. Thamilarasu et al., "A Cross-Layer Based Intrusion Detection Approach for Wireless Ad Hoc Networks," Proc. IEEE Int'l Conf.Mobile Adhoc and Sensor Systems 2005, 2005.

[11] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection in Wireless Ad Hoc Networks," IEEE Wireless Comm., vol. 11, no. 1,pp. 48-60, Feb. 2004.

[12] M. Wang et al., "An Effective Intrusion Detection Approach for OLSR MANET Protocol," Proc. First IEEE ICNP Workshop Secure Network Protocols (NPSec), 2005.