Risk Aware Intrusion Detection and Response Mechanism for MANET

Rama S. Hajari
P. G. Dept., MBES College of Engineering,
Ambajogai, India, 431 517

Veeresh G. Kasabegoudar
P. G. Dept., MBES College of Engineering,
Ambajogai, India, 431 517

ABSTRACT

Mobile Ad-Hoc Networks (MANETS) are dynamic in nature. It is well known fact that dynamic nature of network infrastructure (of MANETS) results in the highly vulnerable to attacks. Among these attacks, routing attack has considerable attention, since it could cause most destructive damage to MANET. A lot of work is going on in the area of Intrusion detection, and response techniques to appease critical attacks. In existing system, binary isolation and DRC techniques are used to isolate the malicious nodes. However, binary isolation leads to unexpected network partitioning and DRC is associative and non-weighted. Therefore, in this paper, we present an adaptive risk-aware response mechanism using CSS-OLSR cooperative security scheme OLSR based on an extended Dempster-Shafer mathematical theory of evidence. The effectiveness of security mechanism is demonstrated by using network simulator NS2 software in which various metrics shows secured performance of the network.

Keywords

Mobile adhoc networks, Intrusion response, Dempster-Shafer theory

1. INTRODUCTION

A mobile ad-hoc network (MANET) is a collection of mobile devices that can communicate with each other without a predefined infrastructure or centralized administration. A MANET can be constructed quickly at a low cost, as it does not rely on existing network infrastructure. Due to this flexibility, a MANET is attractive for many applications like military service, vehicle networks etc.

Recently several efficient routing protocols have been reported in literature. These are classified into two categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as the Ad-hoc On Demand Distance Vector (AODV) [1] protocol, nodes find routes only when required. In proactive routing protocols, such as the Optimized Link State Routing (OLSR) [2] protocol, nodes obtain routes by periodic exchange of topology information. The OLSR protocol is one that offers promising performance in terms of bandwidth and required overhead etc.

In existing system of intrusion response, binary solution or naïve fuzzy response decision technique [3] has been used to isolate to malicious nodes. However these techniques have limitations, where binary responses may result in the unexpected network partition, causing damages to the network infrastructure and naïve fuzzy response could lead to uncertainty in countering routing attacks. In information system L. Sun et al. [4] took D-S theory as a valuable tool for evaluating reliability and security and by other engineering fields [4, 5]. However, Dempster's rule of combination has several limitations [6-9]. In MANET scenario, an improper countermeasure brings additional damages to the network infrastructure [10]. As mentioned in above to overcome these critical issues, more adaptive response should be investigated.

Zhao et al. [10] took Dempster-Shafer mathematical theory of evidence (D-S theory) with importance factors and belief functions and proposed extended Dempster's rule of combination with importance factors (DRCIF). Using this risk aware adaptive decision making module can be created for mitigating MANET routing attacks. This paper presents the implementation of this risk aware response solution with secure OLSR on a simulation.

The rest of the paper is organized as follows: Section 2 overviews a MANET routing protocol OLSR and routing attacks against OLSR. Section 3 presents the details of our risk-aware response mechanism. The simulation results are discussed in section 4. Section 5 concludes this paper.

2. OLSR PROTOCOL

In a MANET the routing protocol discovers the most recent topology of a continuously changing network to find a correct route to a specific node. It requires route discovery as well as route maintenance.

OLSR is a proactive routing protocol for MANET, it is based on periodic exchange of topology information by using link state algorithm. OLSR is an optimization over pure Link State Routing (LSR) protocol [11]. In the OLSR protocols, two types of routing messages are used, a HELLO message and a topology control (TC) message. OLSR reduces the number of transmissions required by using multipoint relay (MPR) to provide an efficient flooding mechanism. In OLSR only nodes selected as MPR nodes are responsible for advertising, as well as forwarding an MPR selector list advertised by other MPRs

3. RISK-AWARE RESPONSE MECHANISM

The cooperative security scheme for OLSR (CSS-OLSR) [12] assures that the nodes correctly generate and relay routing packets. Using this, nodes behaviour can be identified and malicious node can be detected. And, also by using extended Dempster-Shafer theory, Zhao and Ahn [10] proposed new risk-aware response mechanism to systematically cope with the identified routing attacks. This response model considers damages caused by both attacks and countermeasures using them as importance factors.

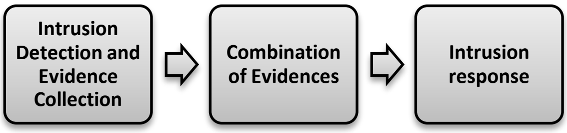

Figure 1: Risk aware intrusion detection and response mechanism

3.1 Intrusion Detection and Evidence Collection

In this step, intrusion detection system identifies the good and bad behaviour nodes by using some additional elements in the regular OLSR protocol as follow:

- Complete Path Message (CPM): when a node receives a TC message it sends a CPM message back to the originator node. The CPM message contains the path traversed by the TC message.[12]
- Rating Table: Each node in the network maintains a rating table which contains three fields, i.e., node ID, primary rating, and secondary rating. For any node with unique node id the secondary rating is classification of node based on direct observation while primary rating is more effective classification based on matching information of CPM message with nodes information announced previously.[12]
- Warning Message: Warning messages are used to notify potential misbehaviour of nodes.[12]

After finding the node as the misbehaving node are the evidences by neighbour nodes which point towards malicious nodes are collected.

3.2 Combination of Evidences

The evidences collected are used to count the risk of attack and risk of countermeasures. Based on the risk of attacks and the risk of countermeasures, the entire risk of an attack is figured out. Suppose EA be the combined evidence for an attack and the combined evidence for a countermeasure be EC. Thus, BelA(Insecure) and BelC(Insecure) represent risks of attack (RiskA) and countermeasure (RiskC), respectively. The combined evidences, EA and EC are defined in (1) and (2). The entire risk value derived from RiskA and RiskC is given in (3)

$E_A = E_1 \oplus E_2 \oplus E_3$ (1)

$E_C = E_4 \oplus E_5$ (2)

Where $\oplus$ is Dempster's rule of combination with important factors [10]

$\text{Risk} = \text{Risk}_A - \text{Risk}_C = \text{Bel}_A(\text{Insecure}) - \text{Bel}_C(\text{Insecure})$ (3)

The algorithm for combination of multiple evidences is constructed as follows [10]:

```
Input: Evidences Ep
Output: One evidence which gives attack alert
1. |Ep| = sizeof(Ep);
2. While |Ep|>1 do
3. Pick two evidences with the least IF in Ep named E1 and E2;
4. Combine these two evidences,
        E= ( $m_1 \oplus m_2$, $(IF_1 + IF_2)/2$);
5. Remove $E_1$ and $E_2$ from Ep;
6. Add E to Ep;
7. End
8. Return the evidence in Ep
```

3.3 Intrusion Response

In this approach, the responses used to deal with different attack methods are routing table recovery and node isolation. Routing table recovery is the first response method after successful detection of attacks. In proactive routing protocols like OLSR, routing table recovery does not bring any additional overhead since it periodically goes with routing control messages [10].

With the output from risk assessment and decision-making module, the corresponding response actions, are carried out to mitigate attack damages in a distributed manner. If the risk of countermeasure i.e. node isolation is greater than risk of attack then no isolation is performed. While if the risk of attack is greater than the risk of countermeasure then node is isolated from the network. If the risks of attack and isolation are nearly equal then a flexible system is used as temporary isolation.

4. SIMULATION RESULTS AND DISCUSSION

The risk aware intrusion detection and response mechanism is implemented using NS2 [13] simulator with UM-OLSR [14]. The simulation parameters for this scenario are shown in table1. In this scenario we measure performance metrics with time variable. Following points may be noted from Figures 2 to 7, and Table 1. As time progresses the attack on routing protocol happens after 60 seconds. So in the figures from 2 to 7 the graphs are plotted after time 60 seconds with different parameters.

- Throughput of the OLSR flow varies as the time changes. As the time increases the average throughput generated decreases. The change in throughput in proposed OLSR protocol with attack and without attack is slightly different. Hence the overhead caused by the attack affect slightly on the routing performance as compared with the normal performance (pl. ref. Figure 2).
- The end to end delay is expressed in second. As the time progresses the average delay is decreased. The delay of proposed OLSR protocol with attack is greater than OLSR protocol without attack (pl. ref. Figure 3).

Table 1: Simulation Parameters

Parameters	Value
No. of nodes	60
Simulation time	100 Sec
Environmental size	1000m*1000m
Traffic type	CBR
Maximum speed	20 m/s
Pause time	2 sec
Source type	MAC

- The jitter is the variation in delay of received packets. It decreases as time progresses. The increased jitter may result in loss of data (pl. ref. Figure 4).

- As the time progresses the packet overhead also increases. The figure 5 shows that the Proposed OLSR protocol with attack has fewer packets overhead than OLSR protocol without attack..Since the routing attack does not change the routing topology the packet overhead is almost same and also it decreases in some cases like this one.
- As the time progresses the number of packets lost also increases. The figure 6 shows the graph of both packets lost in OLSR protocol with attack and without attack. Since the attack causes loss in packets the number of packets lost in proposed OLSR protocol with attack is greater than protocol without attack.

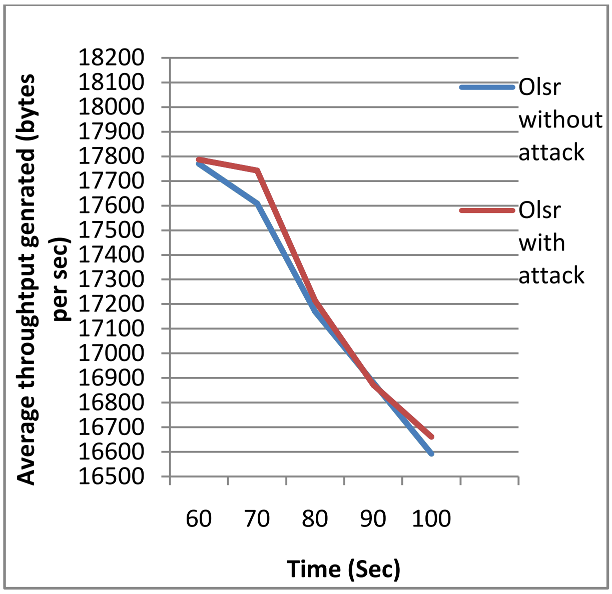

Figure 2: Throughput

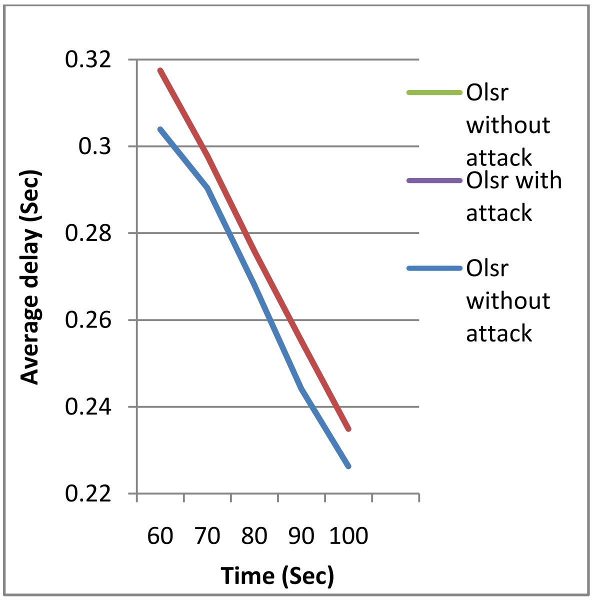

Figure 3: Delay

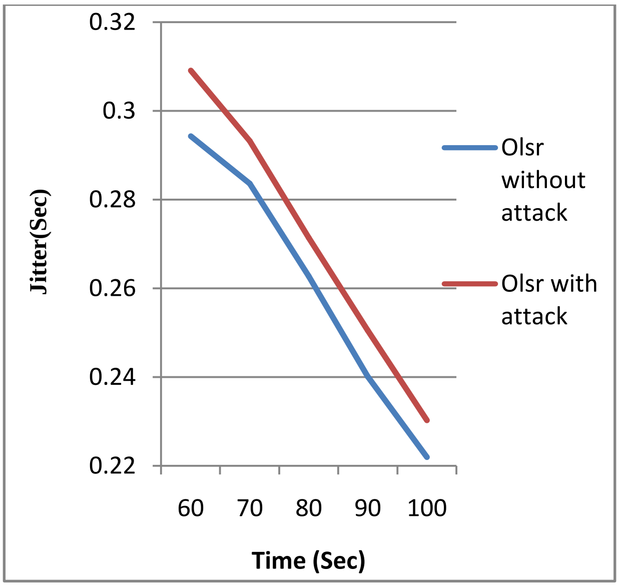

Figure 4: Jitter

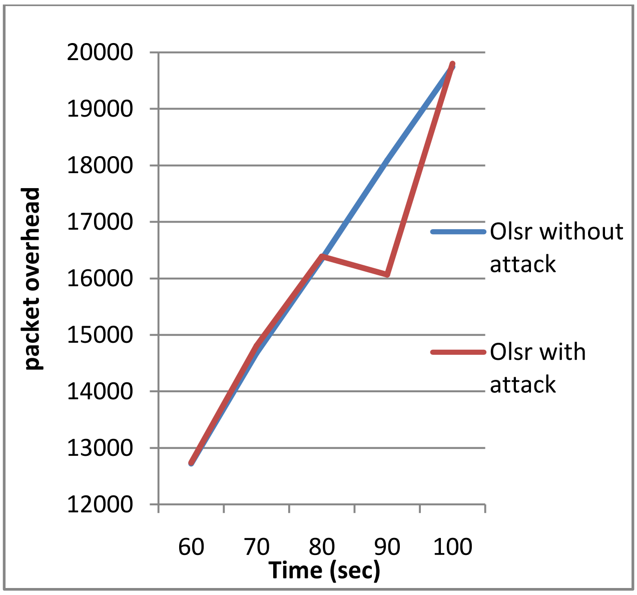

Figure 5: Packet overhead

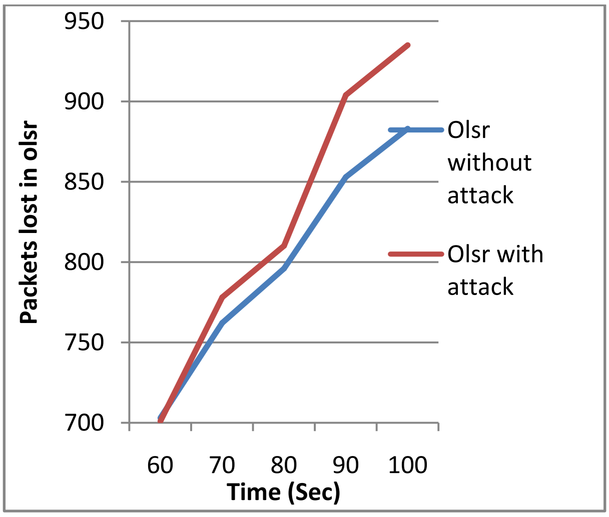

Figure 6: Packet lost

5. CONCLUSIONS

The risk aware intrusion detection and response mechanism is simulated using NS-2.35 network simulator. This approach uses cooperative security scheme in OLSR to identify malicious node. And also it considered the potential damages of attacks and countermeasures. In intrusion response mechanism for node isolating the simple binary isolation sometimes can cause unexpected network partition. With the risk aware approach, the network system is able to balance more damage than attack itself. By using several metrics, we investigated the performance of this approach. Hence, it provides more security in MANET routing. The future work includes inclusion of AODV protocol for comparisons and further improvement in risk detection.

6. REFERENCES

[1] C. Perkins, E. Belding-Royer, and S. Das, "Adhoc on demand distance vector (AODV) routing," *IETF RFC 3561*, July 2003

[2] T. Clausen et. al., "Optimized link state routing protocol," *IETF Internet Draft,* July 2003.

[3] S. Wang, C. Tseng, K. Levitt, and M. Bishop, "Cost-sensitive intrusion responses for mobile adhoc networks," *Proc. 10th Int'l Symp. Recent Advances in Intrusion Detection (RAID '07)*, pp. 127-145, 2007.

[4] L. Sun, R. Srivastava, and T. Mock, "An information systems security risk assessment model under the Dempster-Shafer theory of belief functions," *J. Management Information Systems*, vol. 22, no. 4, pp. 109-142, 2006.

[5] C. Mu, X. Li, H. Huang, and S. Tian, "Online risk assessment of intrusion scenarios using D-S evidence theory," *Proc. 13th European Symp. Research in Computer Security (ESORICS '08)*, pp. 35-48, 2008.

[6] K. Sentz and S. Ferson, "Combination of evidence in Dempster-Shafer Theory," *Technical Report,* Sandia Nat'l Laboratories, 2002

[7] L. Zadeh, "Review of a mathematical theory of evidence," *AI Magazine*, vol. 5, no. 3, p. 81, 1984.

[8] R. Yager, "On the Dempster-Shafer framework and new combination rules_1," *Information Sciences*, vol. 41, no. 2, pp. 93-137, 1987.

[9] H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, "Sensor fusion using Dempster-Shafer theory," *Proc. IEEE Instrumentation and Measurement Technology Conf.*, vol. 1, pp. 7-12,2002.

[10] Z. Zhao, H. Hu, R. Wu and G. Ann, "Risk-aware mitigation for MANET routing attacks", *IEEE transactions on Dependable and Secure Computing*, vol. 9, no. 2, March 2012

[11] C. Adjih, E. Baccelli and P. Jacquet, "Link state routing in wireless ad-hoc networks", *MILCOM2003,* Monterey, CA, Oct 2003.

[12] J. P. Vilela and J. Barros "Daidalos IST Project: Designing advanced interfaces for the delivery and administration of location independent optimised personal services," (FP6-2002-IST-1-506997). http://www.ist-daidalos.org.

[13] K. Fall and K. Varadhan, "The NS manual," 2010.

[14] F. Ros, "UM-OLSR implementation (version 0.8.8) for NS2," 2007.