ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
Research Article
www.ijptonline.com

# QUANTITATIVE RISK ESTIMATION &SOLUTION IN MOBILE AD-HOC NETWORKS

**[1]Mr.Dinto Paul*, [2]Dr B. Raveendranpillai, [3]Mr M G Gireeshan**
[1]Assistant professor in department of ECE,
PRS College of Engg & Technology, Dalumuham Po  Paliyodu Trivandrum-125, Kerala, India
[2]Principal PRS College of Engg & Technology, Dalumuham Po, [3]Research Scientist, Bharath University, Chennai.

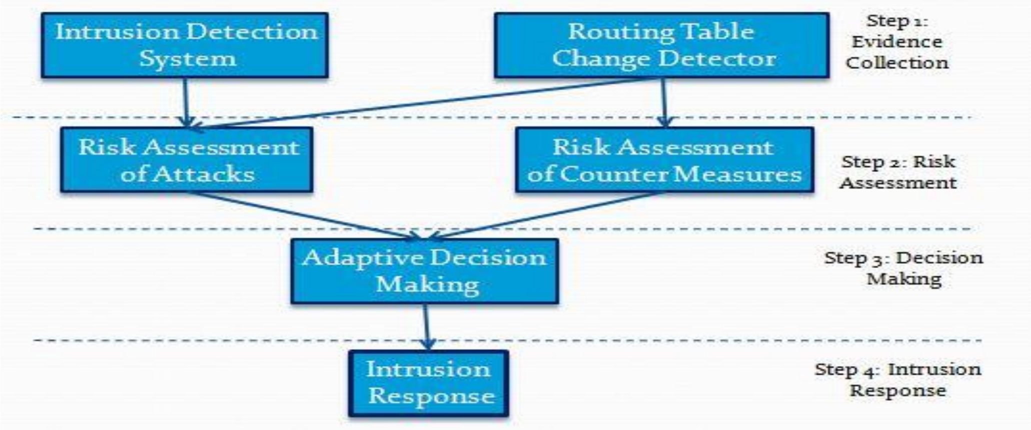
*Received on: 12-02-2017* *Accepted on: 24-03-2017*

## Abstract

The adaptive risk-aware response mechanism is based on quantitative risk estimation and risk tolerance. Instead of applying simple binary isolation of malicious nodes, our approach adopts an isolation mechanism in a temporal manner based on the risk value. Here risk assessment is performed with the extended D-S evidence theory introduced for both attacks and corresponding countermeasures to make more accurate response decisions.

Because of the infrastructure-less architecture of MANET, our risk-aware response system is distributed, which means each node in this system makes its own response decisions based on the evidences and its own individual benefits. Therefore, some nodes in MANET may isolate the malicious node, but others may still keep in cooperation with due to high dependency relationships. This is solved by to introduce a system, which can reduce the routing attacks on mobile adhoc networks and reduce packet loss rate and message tampering which is based on the combination of **Dempster Shafer mathematical** theory and semantic security mechanism. This project also explains the effectiveness of the system by considering various performance factors.

Our risk aware response mechanism is divided into the following four steps shown in Figure.


Intrusion Detection System
Routing Table Change Detector
Step 1: Evidence Collection
Risk Assessment of Attacks
Risk Assessment of Counter Measures
Step 2: Risk Assessment
Adaptive Decision Making
Step 3: Decision Making
Intrusion Response
Step 4: Intrusion Response

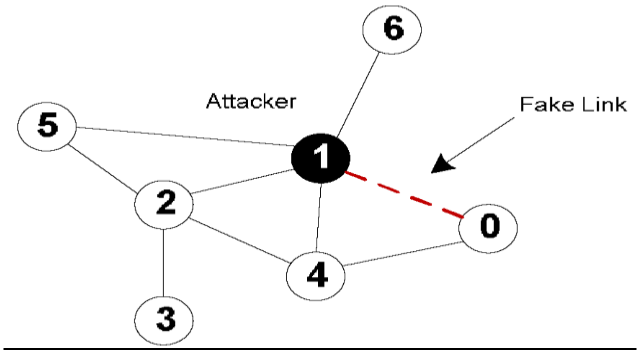
Evidence collection- In this step, Intrusion Detection System (IDS) gives an attack alert with a confidence value, and then Routing Table Change Detector (RTCD) runs to figure out how many changes on routing table are caused by the attack. Risk assessment- Alert confidence from IDS and the routing table changing information would be further considered as independent evidences for risk calculation and combined with the extended D-S theory. Risk of countermeasures is calculated as well during a risk assessment phase. Based on the risk of attacks and the risk of countermeasures, the entire risk of an attack could be figured out.

Decision making- The adaptive decision module provides a flexible response decision making mechanism, which takes risk estimation and risk tolerance into account. To adjust temporary isolation level, a user can set different thresholds to fulfill her goal. Intrusion response- With the output from risk assessment and decision-making module, the corresponding response actions, including routing table recovery and node isolation, are carried out to mitigate attack damages in a distributed manner

In our approach, we use two different responses to deal with different attack methods: routing table recovery and node isolation. Routing table recovery includes local routing table recovery and global routing recovery. Local routing recovery is performed by victim nodes that detect the attack and automatically recover its own routing table.

Global routing recovery involves with sending recovered routing messages by victim nodes and updating their routing table based on corrected routing information in real time by other nodes in MANET.

Node isolation may be the most intuitive way to prevent further attacks from being launched by malicious nodes in MANET. To perform a node isolation response, the neighbors of the malicious node ignore the malicious node by neither forwarding packets through it nor accepting any packets from it. On the other hand, a binary node isolation response may result in negative impacts to the routing operations, even bringing more routing damages than the attack itself.



:

**Example Scenario.**

For example, as in figure Node 1 behaves like a malicious node. However, if every other node simply isolate Node 1, Node 6 will be disconnected from the network. Therefore, more flexible and fine-grained node isolation mechanism are required. In our risk aware response mechanism, we adopt two types of time-wise isolation responses: temporary isolation and permanent isolation.

Evidence selection approach considers subjective evidence from experts' knowledge and objective evidence from routing table modification. We propose a unified analysis approach for evaluating the risks of both attack (Risk A) and countermeasure (Risk C). We take the confidence level of alerts from IDS as the subjective knowledge in Evidence 1. In terms of objective evidence, we analyze different routing table modification cases. There are three basic items in OLSR routing table (destination, next hop, distance). Thus, routing attack can cause existing routing table entries to be missed, or any item of a routing table entry to be changed. We illustrate the possible cases of routing table change and analyze the degrees of damage in Evidences 2 through 5.

Evidence 1: Alert confidence. The confidence of attack detection by the IDS is provided to address the possibility of the attack occurrence. Since the false alarm is a serious problem for most IDSs, the confidence factor must be considered for the risk assessment of the attack.

Evidence 2: Missing entry. This evidence indicates the proportion of missing entries in routing table. Link withholding attack or node isolation countermeasure can cause possible deletion of entries from routing table of the node.

Evidence 3: Changing entry I. This evidence represents the proportion of changing entries in the case of next hop being the malicious node. In this case, the malicious node builds a direct link to this node. So, it is highly possible for this node to be the attacker's target.

Malicious node could drop all the packages to or from the target node, or it can behave as a normal node and wait for future attack actions. Note that isolating a malicious node cannot trigger this case.

Evidence 4: Changing entry II. This evidence shows the proportion of changed entries in the case of different next hop (not the malicious node) and the same distance. We believe the impacts on the node communication should be very minimal in this case. Both attacks and countermeasures could cause this case.

Evidence 5: Changing entry III. This evidence points out the proportion of changing entries in the case of different next hop (not the malicious node) and the different distance. Similar to Evidence 4, both attacks and countermeasures could result in this evidence. The path change may also affect routing cost and transmission delay of the network

## References

1. M. Refaei, L. DaSilva, M. Eltoweissy, and T. Nadeem (2010), "Adaptation of Reputation Management Systems to Dynamic Network Conditions in Ad Hoc Networks," IEEE Trans. Computers, vol. 59, no. 5, pp. 707-719.
2. Y. Sun, W. Yu, Z. Han, and K. Liu (2006), "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 305-317.
3. L. Sun, R. Srivastava, and T. Mock (2006), "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.
4. T. Toth and C. Kruegel (2002), "Evaluating the Impact of Automated Intrusion Response Mechanisms," Proc. 18th Ann. Computer Security Applications Conf. (ACSAC '02), pp. 9-13.
5. H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang (2002), "Sensor Fusion Using Dempster-Shafer Theory," Proc. IEEE Instrumentation and Measurement Technology Conf., vol. 1, pp. 7-12.
6. S. Wang, C. Tseng, K. Levitt, and M. Bishop (2007).,"Cost-Sensitive Intrusion Responses for Mobile Ad Hoc Networks," Proc. 10th Int'l Symp. Recent Advances in Intrusion Detection (RAID '07), pp. 127- 145.