INVESTIGATING THE IMPACT OF ADAPTIVE RISK AWARE RESPONSE SYSTEM WITH DS IMPORTANCE FACTORS IN MANETS


PG Student, ECE Department, JNTU Kakinada, AP, India ¹
Professor, ECE Department, JNTU Kakinada, AP, India ²
Associate Professor, CSE Department, Pragati Engineering College, Kakinada, AP, India ³

Abstract: MANET is a self-organized, infrastructure less network that is established to provide wireless communication in improvised environment. Due to the dynamic network topology, the network is more vulnerable to attacks, predominantly the routing attacks. These routing attacks are detected and the risk level is estimated, for which the necessary response actions are implemented by the Intrusion Response System. Of these response actions, the existing binary isolation and naïve fuzzy deteriorate the network performance when implemented. Hence, in this paper, An Adaptive Risk Aware Response System with Dempster Shafer theory that includes a notion of importance factors (ARSDSIF) is analysed and implemented. In this system, the importance factors are being assigned to evidences to attain the attack frequency and node reputation value of nodes in the network. These parameters (attack frequency and node reputation value) determine the risk threshold to instigate reliable time-wise isolation actions in the network. The ARSDSIF improves the overall network performance when compared to basic intrusion response actions. The effectiveness of our approach is analysed with respect to several performance metrics using NS-2 simulator.

Keywords: MANET, Dempster Shafer theory, importance factors, risk aware response actions

1. INTRODUCTION

Mobile Ad hoc NETwork (MANET) is a set of mobile devices (nodes), which over a shared wireless medium communicate with each other without the presence of a predefined infrastructure or a central authority. The member nodes are themselves responsible for the creation, operation and maintenance of the network. Each node in the MANET is equipped with a wireless transmitter and receiver, with the aid of which it communicates with the other nodes in its wireless vicinity. The nodes which are not in wireless vicinity, communicate with each other hop by hop following a set of rules (routing protocol) for the hopping sequence to be followed. For such networks which were established in improvised environments have the liability to generate security threats. These attacks are due to the compromised nodes in the network. Any compromised nodes under an adversary’s control could cause significant damage to the functionality and security of its network since the impact would propagate in performing routing tasks. Most of the routing protocols proposed for MANETs [4] assume that every node in the network is cooperative and not malicious however the behaviour of nodes can be analysed only by ceaseless supervision of intrusion detection system. There exist a variety of methods like cryptography, authentication etc. that are implemented in Manets. These methods are introduced in Manet, does not consider the effects of intrusion response actions on the network performance. Sometimes may result in unexpected network partition, bringing additional damages to the network. Hence, we consider an adaptive response technique to detect and mitigate with the routing attacks. The technique is based on an extended Dempster-Shafer mathematical theory with notion of importance factors. It involves risk assessment of both intrusions and response actions in Manet which is a nontrivial task due to its involvements of subjective knowledge, objective evidencing and logical reasoning. Subjective knowledge could be gained from previous experience and objective evidence could be attained from observations while logical reasoning requires a formal foundation. In this paper, we make use of Dempster-Shafer mathematical theory of evidence (D-S theory) [14], that offers an alternative to traditional probability theory for representing uncertainty. It accomplishes the task of risk assessment by labelling the evidences with importance factors and belief functions. This mechanism efficiently improves the network performance by detection and appropriate isolation of malicious nodes in the network.

II. RELATED WORK

The primary task of routing protocol is to find the path to ensure that every node acquires a recent map of the network and discover shortest pathway to destinations. Efficient routing protocols have been proposed to handle the dynamic routing traffic in MANET. The major categories of routing protocols are: proactive, reactive and...
hybrid routing protocols. OLSR [12] is the proactive routing protocol selected for performing experiments in this approach after verifying its network performance in the credentials of throughput, end-to-end delay, jitter and overhead. In general, OLSR being a proactive approach has minimal overhead, because messages are broadcasted in the network only through selected MPR nodes. However, if routing attacks occurred in the network like black hole attack, fabrication attack and modification of route replies in the network, there exist worst chances of selecting the malicious nodes itself as the MPR nodes. If that is the case, network experiences serious performance degradation. So, inorder to mitigate such situations, appropriate intrusion detection and response mechanisms have to be adopted to combat with the attacks.

Many research efforts have been made to generate preventive solutions of intrusions [10] for protecting the routing protocols in MANET. However, implementations of these are less hopeful to improve the performance as the response actions may sometimes create involuntary network partition. Numerous intrusion detection systems (IDS) for MANET have been existing and are still the active research area. Due to the nature of MANET, most IDS designed are distributed in nature and have a cooperative architecture. As signature-based and anomaly-based IDS models are used for wired network, IDS for MANET use specification-based approaches and statistics-based approaches. Specification-based approaches, for example DEMEM, supervises the network activities and compare them with known attack features, however they failed to combat with new attacks. On the other side, statistics-based approaches, for example Watchdog and Lipad, compare existing network activities with normal behaviour patterns, which result in higher false positives rate than in the specification-based approaches. Because of the false positives in both MANET IDS models, intrusion alerts generated from these models always accompany with some confidence value, which signifies the possibility of attack occurrence.

Intrusion alerts that are utilised in our paper are node reputation value and attack frequency. Any deviation from the threshold value generated by these attack alerts is noted, intrusion response systems (IRS) will implement isolation of malicious nodes. Response actions like naive fuzzy responses and simple binary isolation will take advantage of IDS alerts but involuntary isolation of nodes may cause unexpected network partition. This brings the concept of cost-sensitive MANET intrusion response approach which considers topology dependency and attack damage. The advantage of our solution is that we integrate evidences from IDS to attain a combined evidence for all the local routing table changes and utilises expert knowledge to estimate risk of both attacks and countermeasures with a mathematical reasoning approach like Dempster Shafer theory. This approach involves differentiating and prioritizing different evidences in terms of security and criticality.

III. EXTENDED DEMPSTER SHAFER THEORY OF EVIDENCE

D-S theory is a prominent methodology for investigating reliability and security in most of the upgraded information systems and other engineering fields, where accurate calibration is difficult. D-S theory is characterized by the following:

1) It provides a way to represent both subjective and objective evidences with basic probability assignment and belief function.
2) It utilises Dempster’s rule of combination (DRC) inorder to combine different evidences that are gathered with reasoning in steps.
3) New Extended Dempster’s Rule of Combination with a notion of Importance Factors (IF) treats evidences by differentiating and prioritizing among them based on the attack alerts.
4) This approach considers risk factor caused by both intrusions and response actions.

The adaptiveness of this approach allows to effectively combat with MANET routing attacks.

In this paper, risk-aware response mechanism is implemented with extended Dempster Shafer theory with above stated characteristics. This helps to efficiently combat with attacks in MANET by effective intrusion detection and implementation of adaptive time-wise isolation method. In order to evaluate the efficiency of our mechanism, we perform a series of simulated experiments with a proactive MANET routing protocol, Optimized Link State Routing Protocol (OLSR) using NS-2.34 simulator.

A. Importance Factors

In D-S theory, propositions are represented as subsets of a given set. When a proposition corresponds to a subset of a frame of discernment, it implies that a particular frame discerns the proposition. First, we introduce a notion of importance factors

1) Definition 1: Importance factor (IF) is a positive real number associated with the importance of evidence. Ifs are derived from historical observations or expert experiences.

2) Definition 2: An evidence E is represented by a 2-tuple (m, IF) where m describes the basic probability assignment function and IF represents the importance factor.

B. Belief Functions

If Bel1 and Bel2 are two belief functions over the same frame of discernment [3], with basic probability assignments m1 and m2 of those respective evidences and the importance factors of these evidences as IF1 and IF2. Also the function m defined by our proposed DRCIF is weighted and non associative for multiple evidences. Hence if the sequential information is not available for
some instances, it is appropriate to make the combined evidence consistent with multiple evidences.

Extended D-S evidence model with importance factors in this approach is as follows: Suppose \( E_1 = (m_1, IF_1) \), \( E_2 = (m_2, IF_2) \) are two independent evidences with \( m_1, m_2 \) as basic probability functions of respective evidences and \( IF_1, IF_2 \) as the importance factors of those evidences. Then, the combined evidence \( E \) of \( E_1 \) and \( E_2 \) is:

\[
E = (m_1 \oplus m_2, (IF_1 + IF_2)/2),
\]

where \( \oplus \) is Dempster’s rule of combination with importance factors. Our combination algorithm supports the requirement and the complexity of our algorithm is extended up to \( n \) evidences represented by \( O(n) \), where \( n \) is the number of evidences. This indicates that approach of extended Dempster-Shafer theory expects no extra computational cost compared to a naive fuzzy-based method.

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

Algorithm : One evidence
1) \( |Ep| = \text{size of (Ep)} \);
2) While \( |Ep| > 1 \) do
3) Pick two evidences with the least IF in Ep, named \( E_1 \) and \( E_2 \);
4) Combine these two evidences,
   \[
   E = (m_1 \oplus m_2, (1IF_1 + 1IF_2)/2);
   \]
5) Remove \( E_1 \) and \( E_2 \) from \( Ep \);
6) Add \( E \) to \( Ep \);
7) End

The Evidences are collected by the IDS and priorities assigned to each of them by means of importance factors on the basis of attack alerts such as attack frequency and node reputation value of nodes in the network. Risk assessment is done for both attacks and their counter measures. Adaptive decisions are taken on the basis of the node behaviour i.e. attacker or not by comparing with the threshold values namely upper risk tolerance and lower risk tolerance. Finally, Intrusion response system will send an alert to all nodes in the network for updation of changes in the routing table.

### IV. Risk Aware Response Mechanism

In this section, an adaptive risk-aware response mechanism [1] as represented in figure 1, is explained that implements adaptive response actions based on quantitative risk estimation and risk tolerance values. Instead of applying simple binary isolation of malicious nodes, this approach adopts an isolation mechanism in a temporal manner based on the risk value.

#### A. Response to routing attacks

In risk aware approach, implementation of two different responses is done to combat with different attacks. They are: Routing table recovery and Node isolation.

#### B. Risk assessment

Since the response actions after successful detection of intrusions may cause further damages than the attacks itself; hence the risk of both attacks and counter measures should be considered. The security states of MANET are...
under the two categories: (Secure, Insecure). In other words, the frame of discernment [3] would be \{φ, (Secure), (Insecure), (Secure, Insecure)\}. Where Bel\{Insecure\} is used to represent the risk of MANET whereas Bel\{Secure\} is used to represent the secured state of MANET.

1) **Evidences Selection:** A unified analysis approach for analysing the risks of both attack (Risk\_\alpha) and countermeasure (Riskc) is implemented. We consider the confidence level of alerts from IDS as the subjective knowledge. For objective knowledge, we consider different routing table modification cases. The routing attack can cause the following changes i.e. existing routing table entry to be missed, or any item of routing table entry to be changed. We illustrate the cases of routing table changes and analyse the degrees of damage from evidences.

2) **Combination of evidences:** The combined evidence for attacks is $E_{\alpha}$ and the combined evidence for countermeasures is $E_{c}$. Thus, Bel\{Insecure\} and Bel\{Insecure\} represent risk of attacks (Risk\_\alpha) and risk of countermeasures (Riskc), respectively.

\[
\text{Overall Risk} = \text{Bel\{Insecure\}} - \text{Bel\{Insecure\}}
\]

**C. Adaptive Decision making**

Adaptive decision making module [6] is dependent on quantitative risk estimation and risk tolerance. The response actions in decision making are divided into multiple bands. Each band is allotted with an isolation degree that presents a different time period for isolation action. The response actions and isolation band boundaries are all decided based on risk tolerance and can be changed when risk tolerance threshold changes. The upper risk tolerance threshold ($UT$) would signify permanent isolation response whereas the lower risk tolerance threshold ($LT$) would signify no isolation at all i.e. it maintains each node intact. The band lying between the upper tolerance threshold and lower tolerance threshold is associated with the temporary isolation response, in which the isolation time ($T$) varies instantaneously. Isolation band, $i$ is based on the response level where $n$ is the number of bands and $i$ is the corresponding isolation band.

\[
i = \frac{\text{Risk} - \text{LT}}{\text{UT} - \text{LT}} \times n, \text{Risk} \in (\text{LT, UT})
\]

\[
T = 100x i \text{ (milliseconds)}
\]

Decision making is based on the risk tolerance threshold and implements the following three levels of isolation.

- **Risk tolerance thresholds** will also be dynamically varied by alerting values, such as attack frequency and node reputation value [9]. If the attack frequency is more, severe response actions i.e. permanent isolation will be implemented to counteract the attack. Implemented risk-aware response approach could achieve the isolation of appropriate malicious nodes temporarily and permanently basing on risk factor estimated and narrowing the range between upper and lower risk tolerance thresholds.

1. **No isolation:** The lower risk tolerance threshold ($LT$) would result in no isolation and all the nodes in network as such.
2. **Temporary isolation:** If the risk level falls between the lower risk tolerance thresholds ($LT$) and higher risk tolerance threshold ($HT$), the appropriate response action implemented would be temporary isolation.
3. **Permanent isolation:** If the risk level is above the higher tolerance threshold ($HT$), the decision would be permanent isolation of node.

**V. SIMULATION SETUP**

MANET scenarios are generated in NS-2 that are constructed with a topology of 50 nodes with 750m×750m terrain region. In the conducted experiments, OLSR routing protocol is employed which outperforms other routing protocols in different data traffic models in different performance metrics [15] as it is basically a table driven protocol. The total simulation time was set to 1,200 seconds. Constant Bit Rate (CBR) traffic was used to send 512 byte-UDP packets between nodes. The queuing capacity of every node was set to 150. We adopted a random traffic generator in the simulation that chose random pairs of nodes and sent packets between them. Every node kept track of all packets sent by itself and the entire packet received from other nodes in the network.

**A. Performance Evaluation**

In order to evaluate the effectiveness of our adaptive risk aware response solution, we compared the network performance internms of six metrics.

**Packet delivery ratio:** The ratio between the number of packets originated by the application layer CBR sources and the number of packets received by the CBR sink at the final destination.
When the number of attacker nodes is rising from 0-6, the performance of both approaches remained equal, however figure 3 illustrates that after 6 nodes the performance of DRC is degrading drastically and when the DRCIF is implemented, packet delivery ratio is improved to a considerable extent. This is due to the fact that there exists more routing choices for the packets to be delivered in DRCIF scheme.

2) **Routing cost**: The ratio between the total bytes of routing packets transmitted during the simulation and the total bytes of packets received by the CBR sink at the final destination.

From figure 4, it is clear that the performance of DRCIF is consistently decreased when compared to DRC with varying attacker nodes from 0-10. Routing cost for the proposed DRCIF is reduced since the method is a statistical approach that better analyses and predicts the number of hops included.

3) **Control overhead**: The number of transmitted routing packets; for example, a HELLO or TC message sent over four hops would be counted as four packets in this metric.

From figure 5, it is observed that the overhead of proposed DRCIF scheme is predominantly low when compared to DRC system, due to instigation of appropriate time wise isolation of nodes in the methodology, and the number of nodes permanently isolated is also very low when compared to binary isolation and naive fuzzy schemes.

4) **Mean latency**: The average time elapsed from “when a data packet is first sent” to “when it is first received at its destination.”

Figure 6 shows that mean latency period is also reduced to noticeable extent in the proposed DRCIF scheme with the variation of attacker nodes from 0 to 10.

5) **Energy consumption**: The amount of energy consumed from initial state to final state during the transmissions by nodes in the network.
Energy consumption in MANET scenario is high as the nodes are mobile nature. Residual energy in nodes is reduced with the increased number of attacker nodes in the network. However, from figure 7, we observe that the energy remained in the nodes is comparatively high in the DRCIF scheme when compared to existing DRC scheme, as the impact of attackers is lowered by subsequent detection and implementation of response actions in the network.

VI. Conclusions
In this project, risk-aware response solution has been proposed for mitigating MANET routing attacks. The routing attacks in the network have been identified based on the performance variation. This D-S mathematical model has been implemented to identify the possibility of the attack occurrence in the network. Thus, the consideration of the potential damages of attacks and countermeasures have been identified and reduced. In order to measure the risk of both attacks and countermeasures, an extended Dempster-Shafer theory of evidence with a notion of importance factors based on the node reputation value, historical observations and expert experiences. Based on several performance metrics, the network performance has been estimated and compared it with the existing system. We also investigated the performance and practicality of our approach and the experiment results clearly demonstrated the effectiveness and scalability of our risk-aware approach. Based on the performance results obtained through these work, we better analysed the frequency of the attack occurrence in the network.

Acknowledgement
I am very thankful to our Prof. Dr. B. Prabhakara Rao and Assoc prof. B.A.S. Roopa Devi for their consistent support and guidance throughout the project period. I acknowledge the support of my peers who supported me in this work.

References

Biographies
B Satya Sravani has completed her B.E. in Electronics and Communication Engineering from Regency Institute of Technology, Pondicherry University, Puducherry, India in the year 2012. She is currently pursuing her Master’s Degree program in Computers and Communication Engineering in J.N.T. University Kakinada, A.P., India..

Dr B Prabhakara Rao obtained B.Tech & M.Tech from S.V. University, Tirupathi with Specializations in Electronics and Communications Engineering. Electronic Instrumentation and Communications Systems in the years 1979 and 1981 respectively. He received the Doctoral degree from Indian Institute of Science, Bangalore in the area of Sonar Signal processing in the year 1995. Currently, he is the senior professor in Electronics and Communication Engineering in J.N.T. University, Kakinada, A.P., India.