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

RELATION BETWEEN ADHOC NETWORKS &DEMPSTER SHAFER MATHEMATICAL THEORY

Mr.Dinto Paul*
Assistant professor in department of ECE,
PRS College of Engg & Technology, Dalumuham Po Paliyodu Trivandrum-125, Kerala, India.

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

Abstract

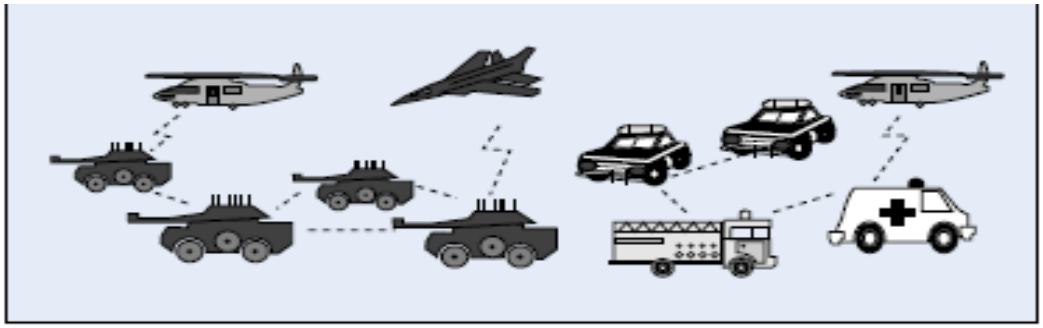
Mobile ADHOC networks are extremely prone to attacks due to the sophisticated nature of its network structure. Among these attacks routing attacks have received considerable attention since it could cause the most severe damage to MANET. Though there are so many intrusion response techniques to reduce such attacks, existing solutions typically attempt to isolate malicious nodes based on binary responses however, binary response may result in the unexpected network partition, causing further damage to the network infrastructure and could lead to problems in managing routing attacks in MANET. This project is intended 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.

Mobile Ad Hoc Network

The wireless networks have become increasingly popular in the communication industries and it provides mobile users with ubiquitous computing capability and information access regardless of the users' location. There are currently two variations of mobile wireless networks: infrastructure and infrastructure less networks.

The infrastructured networks have fixed and wired gateways or the fixed Base-Stations which are connected to other Base Stations through wires. Each node is within the range of a Base-Station. A "Hand-off" occurs as mobile host travels out of range of one Base-Station and into the range of another and thus, mobile host is able to continue communication seamlessly throughout the network. Example applications of this type include wireless local area networks and Mobile Phone. The other type of wireless network, infrastructure lessnetworks, is knows as Mobile Ad-hoc Networks(MANET).

A MANET networks have no fixed routers, every node could be a router. All nodes are capable of movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. The entire network is mobile, and the individual terminals are allowed to move freely. In this type of networks, some pairs of terminals may not be able to communicate directly with each other and have to rely on some terminals so that the messages are delivered to their destinations. Such networks are often referred to as multi-hop or store-and forward networks. Those networks provide mobile users with ubiquitous communication capability and information access.



Example for applications of MANET

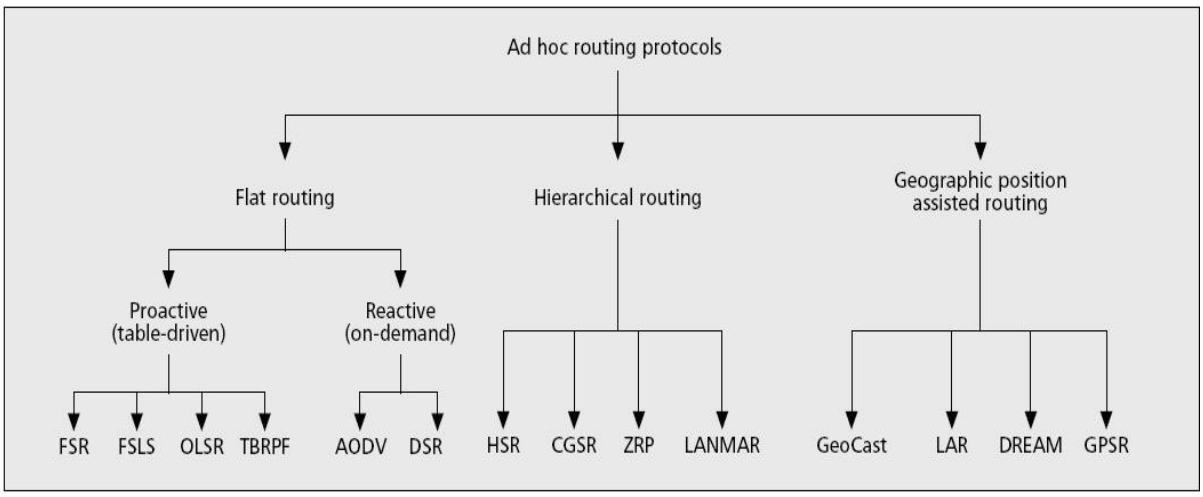
Some of the main features of MANET are listed as:

a) MANET can be formed without any preexisting infrastructure.

b) It follows dynamic topology where nodes may join and leave the network at any time and the multi-hop routing may keep changing as nodes join and depart from the network.

c) It does have very limited physical security, and thus increasing security is a major concern.

d) Limited Bandwidth & Limited Power.



Classification of Routing Protocols in Mobile Ad-hoc Networks

The nodes of the network work as the routers to the packet data and transmit it from one node to another till the destination. These nodes are mobile and can be located on ship, car, bus or aero plane. As the data has to pass several nodes before getting delivered a routing protocol is must so that data can be passed from one node to another and delivered to the correct address. Routing protocols are classified into six categories according to the way they perform their work and we will discuss two of them Reactive and Proactive Protocols.

Mobile Ad hoc Networks (MANET) have been highly vulnerable to attacks due to the dynamic nature of its network infrastructure. Among these attacks, routing attacks have received considerable attention since it could cause the most devastating damage to MANET. Even though there exist several intrusion response techniques to mitigate such critical attacks, existing solutions typically attempt to isolate malicious nodes based on binary or naı¨ve fuzzy response decisions. However, binary responses may result in the unexpected network partition, causing additional damages to the network infrastructure, and naı¨ve fuzzy responses could lead to uncertainty in countering routing attacks in MANET. However Dempster's rule of combination has several limitations, such as treating evidences equally without differentiating each evidence and considering priorities among them. To address these limitations in MANET intrusion response scenario, we introduce a new Dempster's rule of combination with a notion of importance factors (IF) in D-S evidence model.

In this paper, we propose a risk-aware response mechanism to systematically cope with routing attacks in MANET, proposing an adaptive time-wise isolation method. Our risk-aware approach is based on the extended D-S evidence model. In order to evaluate our mechanism, we perform a series of simulated experiments with a proactive MANET routing protocol, Optimized Link State Routing Protocol (OLSR).

The major contributions of this paper are summarized as follows:

Here an extended D-S evidence model with importance factors and articulate expected properties for Dempster's rule of combination with importance factors (DRCIF) is proposed. Our Dempster's rule of combination with importance factors is nonassociative and weighted, which has not been addressed in the literature.

An adaptive risk-aware response mechanism with the extended D-S evidence model, considering damages caused by both attacks and countermeasures is proposed. The adaptiveness of our mechanism allows us to systematically cope with MANET routing attacks.

References

1. P. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, and A. Reninger (2007), "Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control," Proc. 28th IEEE Symp. Security and Privacy.
2. H. Deng, W. Li, and D.Agrawal (2002), "Routing Security in Wireless Ad Hoc Networks," IEEE Comm. Magazine, vol. 40, no. 10, pp. 70- 75.
3. J. Felix, C. Joseph, B.-S. Lee, A. Das, and B. Seet (2011), "Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA," IEEE Trans. Dependable and Secure Computing, vol. 8, no. 2, pp. 233-245.
4. Y. Hu, A. Perrig, and D. Johnson (2002), "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM, vol. 3, pp. 1976-1986.
5. Y. Hu and A. Perrig (2004), "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security and Privacy Magazine, vol. 2, no. 3, pp. 28- 39.