Detection and Avoidance of Routing Attack in Mobile Ad-hoc Network using Intelligent Node

Abhiskek Ranjan, Venu Madhav Kuthadi, Rajalakshmi Selvaraj, and Tshilidzi Marwala

***Abstract*—** the routing attacks are created in order to damage the network in Mobile Ad-hoc. Previously, Dempster-shafer theory introduced a solution for these routing attacks where it entirely works on the principle of Dempster rule with various important factors to mitigate these critical routing attacks. Previously the system contains an Intrusion detection mechanism which is used to create a message whenever the attacker attacks the network. This Intrusion detection system sends an alert message to each mobile node in the network, when the attacker attacks the network. Then, Routing table change Detector identifies exactly how many changes has occurred in each node after receiving the alert messages from the intrusion detection system and also it make some changes in the routing table of each node in the network. From these changes, the Intrusion detection system identifies the attackers and these attackers are isolated from the network. The main drawback of this existing system is whenever the attacker is occurred, the Intrusion detection system has to send an alert message every time and the routing table change detector has to make some changes in the routing table. In order to avoid these drawbacks, the knowledge based intelligent system is proposed. In this proposed system, initially a source node has to get an authorized path from the intelligent node (a node with high energy) to send a data to the destination node. This proposed system discussed with the four routing attacks such as route salvage, sleep deprivation, colluding miss relay and collision attack.

***Keywords*—** Dempster-shafer theory, attacker, route salvage, sleep deprivation, colluding.

I. Introduction

RECENT advances in computer networking have introduced a new technology for future wireless communication, a mobile ad hoc network (MANET). This new technology (MANET) is the combination of peer-to-peer techniques, wireless communications and mobile computing which provides a convenient infrastructure-less communications. This technology is also very useful to provide communications for Many applications especially when the infrastructure networks are not feasible.

Abhiskek Ranjan, Faculty of Engineering and the Built Environment University of Johannesburg South Africa.

Venu Madhav Kuthadi, Department of AIS Faculty of Management University of Johannesburg South Africa.

Rajalakshmi Selvaraj, Department of Computer Science Botswana International University of Science and Technology, Gaborone, Botswana

Tshilidzi Marwala, Faculty of Engineering and the Built Environment University of Johannesburg South Africa.

MANET can be used to overcome geographical constraints in a military operation. As MANET is very easy to deploy, it may also very useful to assist in the disaster relief operations where temporary network infrastructure is immediately needed to replace the damaged infrastructure networks.

Moreover, MANET is also vulnerable to many security attacks which are similar to other networks. MANET not only inherits all the security threats which is faced in both wired and wireless networks, but it also introduces security attacks which is unique to itself [1]. As people are encouraged to use a secured network, it is important to provide MANET with reliable security mechanisms which can be widely used for next few years. Before the development of any security measure in order to secure mobile ad hoc networks, it is very important to study the variety of attacks which is relevant to such networks. With the knowledge of some common attack issues, researchers have a better understanding about how mobile ad hoc networks is threatened by the attackers and thus it leads to the development of more reliable security measures in protecting them.

In this paper, an intelligent node is proposed which can distribute the key to each mobile node in the network in order to avoid attacks. During the network formation, each node is aware of their key in the network. The rest of this paper is organized as follows: Section 2 describes related work. Section 3 describes Routing attack against MANET Section 4 describes about the proposed system Section 5 describes about the Conclusion of this paper.

II. Related Work

More number of investigations have been investigated to provide preventive solutions for this attacks and these solutions are used to protect the routing protocols in Mobile Ad-Hoc Network [7], [8], [9], [10]. These methods are useful in protecting the attacker node from joining with the network and also to establish an important overhead for the process of key verification and key exchange process with the restricted interruption elimination. Additionally, prevention based techniques are not useful to handle with the attacker node, which have valid credentials to communicate with the network.

More number of Intrusion Detection System is introduced newly for MANET. Naturally, the most Intrusion Detecting Systems are planned to distribute and also it has a cooperative architecture in the MANET which is similar to the Anomaly based Intrusion Detecting Systems and signatures-based Intrusion Detecting Systems to wired network. MANET

employ statistic based or specification based methods to Intrusion Detecting Systems. For instance, DEMEM specification method [11] and [12], [13], [14], these approaches initially checks the network activities and then it compares them with already identified attack features. These are impossible to manage with new attacks. Alternatively, statistics-based approaches like as Watchdog [15] [16] matches the network actions with normal activities patterns. Then the outcome is high false positive rate than specification-based approach. Due to the reality of false positives in both of the MANET Intrusion Detecting Systems models, the alert confidence is always coming with these systems such as intrusion alerts where it specifies the chances of attack occurred in the MANET.

IRS (Intrusion response system [17]) for MANET is stimulated by MANET Intrusion Detecting Systems. Basically, the malicious nodes are remote by their reputations [1], [2]. The malicious node's job fails to obtain advantage of Intrusion Detecting System alerts and also a simple isolation can cause unpredicted network division. The cost-sensitive intrusion response concept considers both attack damage and topology dependency which is brought by Wang et al. [4]. The benefits of Dempster model are to combine the counter measures with the mathematical reasoning approach as well as local routing table, Intrusion Detecting System with the expert knowledge. Risk-aware approaches [18], [19]: These approaches are used to make the response decisions and it is based always on the already exists inherent uncertainty. It leads to irregular risk, especially in intelligence area and security. So to tackle this kind of problems, the risk aware approach is introduced with the corresponding advantages and damage tradeoffs. Adaptive risk-based access control is presented in Cheng et al. [3] for a fuzzy logic control method. To decide whether an access to the network must be permitted or denied by dynamic risk-aware method is presented in Teo et al [20].

But, still now risk assessment is nontrivial challenging problem due to its involvement of objective evidence, subjective knowledge, and logical reasoning. A naıve fuzzy cost-sensitive intrusion response method is used by Wang et al [4]. These cost methods are taken as objective evidence and subjective knowledge into account. But, it replaced a seamless joining of two assets with logical reasoning. In [5] Dempster-Shafer principle is used to measure the risk of attacks.

III. Routing Attacks Against Manets Protocols

A. Route salvaging attacks

Route salvaging attacks are launched by the greedy internal nodes in the networks. Generally in mobile ad hoc network, there is no proper assurance that each transmitted packet will effectively reach the preferred destination node. As the adversaries make attack in the network and possible network failures can cause the packet to be damaged. Hence, to salvage the packets from such failures, misbehaving internal nodes might duplicate and retransmit their packets even though no-sending-error messages are received. If many greedy nodes exist in the network, those nodes will make severe route salvaging attacks. In addition to the demand of resources in destination nodes and intermediate, route salvage attack may also consume unnecessary bandwidth.

B. Sleep depreciation attack

This type of attack is more particular in MANET. The attacker node makes the path node busy by sending the unnecessary packets to it. Hence the battery power of path node is drained off unnecessarily. With the aid of unnecessary routing packets flooding, the targeted node launches the sleep deprivation attacks in the network. By sending a large number of route replies (RREP) or route error (RERR), routing request packet, the attackers can damage the targeted node (path node) in the network. This makes the affected node to become unreachable and incapable of participating in the routing mechanism in the network.

C. Colluding Miss Relay Attack

In order to interrupt the routing operation in a MANET, several attackers participate in collusion drop or modify the packets. The conventional methods such as path rater and watchdog are facing difficulties in the detection of these attacks. The figure.1 shows an instance of this attack. Assume the case where node A1 sends packets for node T as illustrated in figure a. where the routing packets are forwarded by A1 in order to avoid being noticed by node T. However, the next attacker A2 modifies or drops these routing packets.

D. Wormhole Attack

In the Wormhole attack figure.2 a tunnel giving an illusion that they are neighbor and connects two colluding nodes that are far apart. Each of these nodes receive route request and topology control messages from the network and send it to the other colluding node via tunnel which will then replay it into the network. By using this additional tunnel, these nodes are able to advertise that they have the shortest path through them. Once this link is established, the attackers may choose each other as multipoint relays (MPRs), which then lead to an exchange of some topology control (TC) messages and data packets through the wormhole tunnel. Since these MPRs forward flawed topology information, it results in spreading of incorrect topology information throughout the network [6]. Figure describes it with two nodes X and Y. In the figure, node A and B are 3hop away from each other. And attacker node X and X' shows that they are neighbor of A and B respectively. So they make the tunnel between node A and B, and they can drop the packet received from A or B.

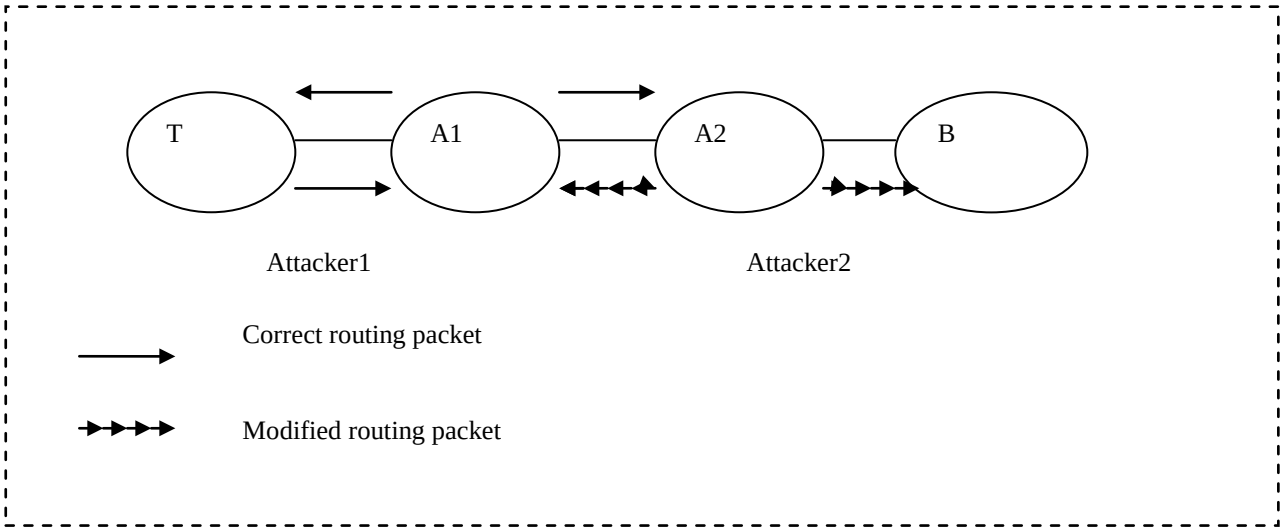

Fig. 1 Colluding Miss relay Attack

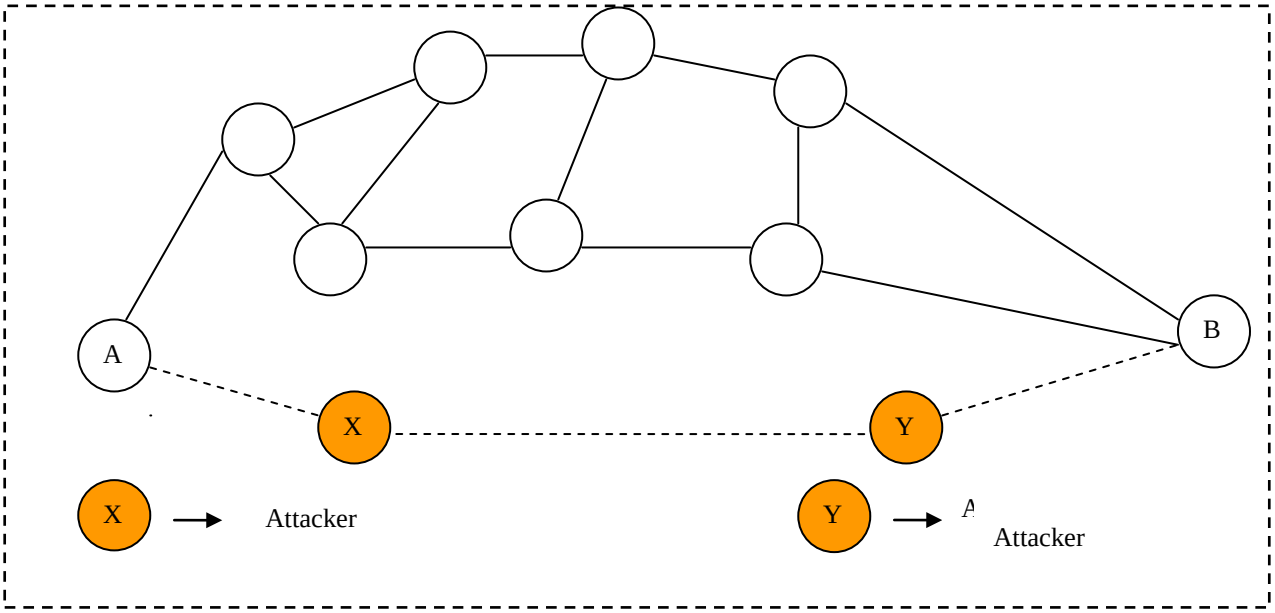

Fig. 2 Wormhole attack

IV. Proposed System

In proposed system, mobile nodes are trained during the time of network creation. With the help of energy calculation, the node with highest energy is considered as intelligent node. The main task of this intelligent node is to distribute the key to entire mobile nodes in the network, in order to train the nodes. Thus the nodes in the network are trained. Whenever the intelligent node sends key request to mobile node, the already trained mobile nodes reply to the intelligent node queries while the attacker node couldn't reply to the intelligent node as the attacker node does not aware about the key. The four types of attacks are handled by intelligent node itself. Those attacks are route salvage attack, sleep depreciation attack, colluding miss relay attack and worm whole attack.

In proposed system, the mobile nodes are trained when the network is deployed. If a source node needs to send the packet to the destination node, it has to request the authorized path to the intelligent node. Then the intelligent node sends key request to all the nodes in the network. After receiving the key request, the mobile node sends key reply to the intelligent node request as the nodes are already trained. But the attacker node in network couldn't reply to the intelligent request as it is not aware of the key. Finally the authorized path is found by the intelligent node and the intelligent node reply to the source node. With the help of this discovered authorized path, the data transfer will takes place. The source node sends key request to path node, after receiving key reply from the path node the source node send packet to the path node. The same process will be repeated, until the packet reaches its destination. Thus, the packet transmission will be secured. As discussed earlier, the routing attacks create a significant damage to MANET network. These routing attacks are completely avoided with the aid of knowledge based intelligent node

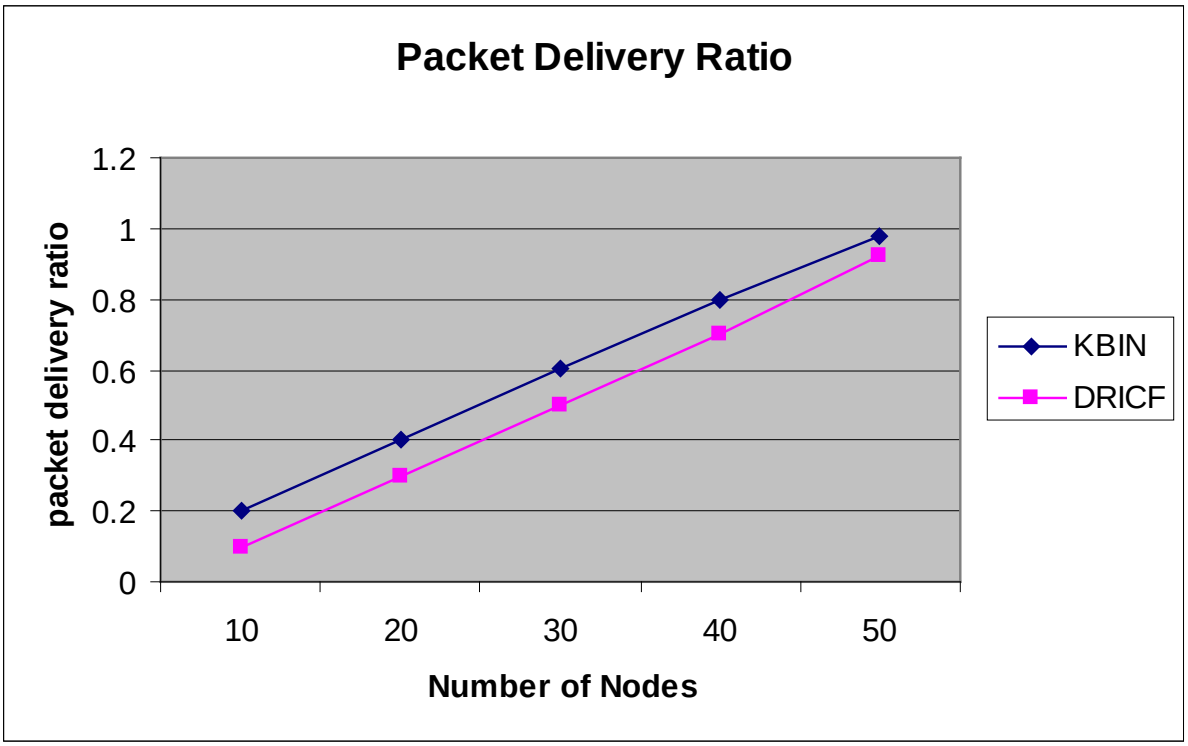

Fig. 3 Packet Delivery Ratio among DRCIF and KBIN

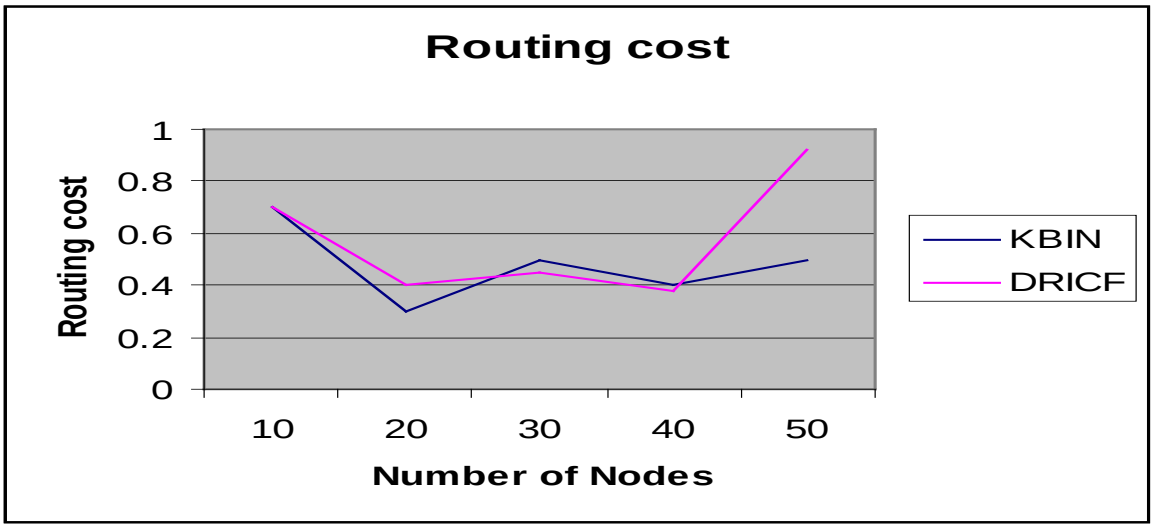

Fig. 4 Routing Cost among DRCIF and KBIN

V. Performance Of Proposed System

In order to test the scalability and efficiency of our proposed system, KBIN (knowledge based intelligent node) is evaluated in this section. Consider 10, 20, 30, 40, and 50 nodes respectively. As illustrated in Fig. 3, when the number of nodes increases, the packet delivery ratio also increases because there are more route choices available for the packet transmission.

In Fig. 4, it is observed clearly that the routing cost of our proposed system is lower than that of the other DRICF. Note that the random traffic generation and random placement of nodes in our realistic, cause the fluctuations of routing cost shown in Fig. 4 simulation. As shown in Fig. 5 and Fig.6, notice that as the number of nodes increases, the packet overhead and the byte overhead using our KBIN results are slightly higher than that of the other DRICF. In Fig. 7, the mean latency using our KBIN is higher than DRCIF. Particularly in route salvage and sleep depreciation attack the power and bandwidth are affected, but using proposed mechanism a higher result than that of the DRICF is achieved, which is illustrated in Fig. 8 and Fig.9 respectively.

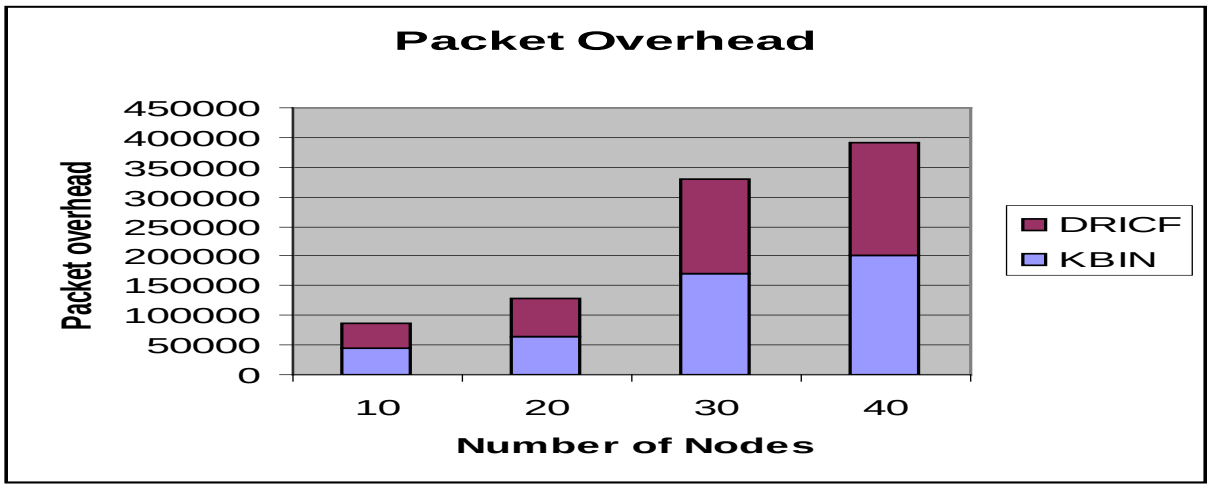

Fig. 5 packet overhead among DRCIF and KBIN

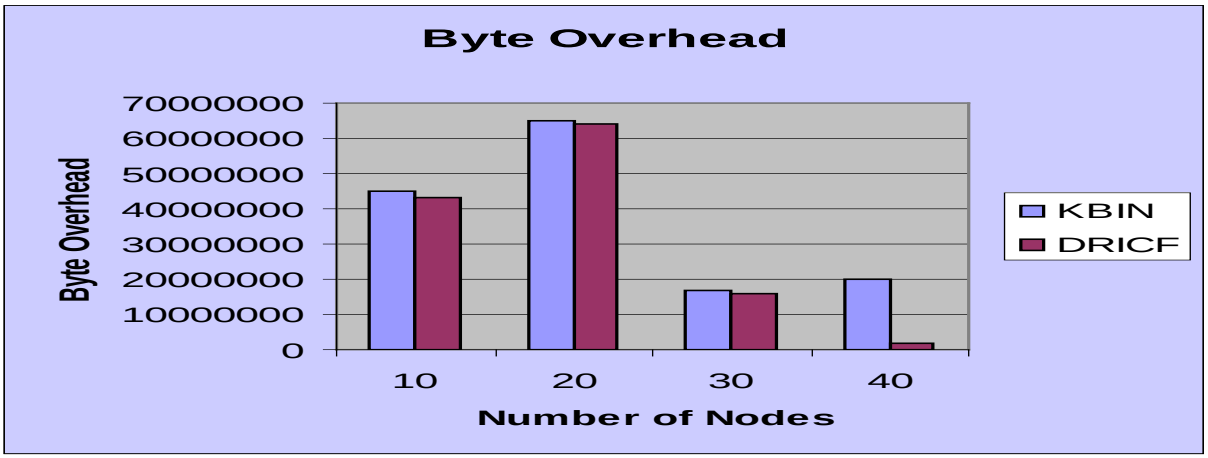

Fig. 6 Byte Overhead among DRCIF and KBIN

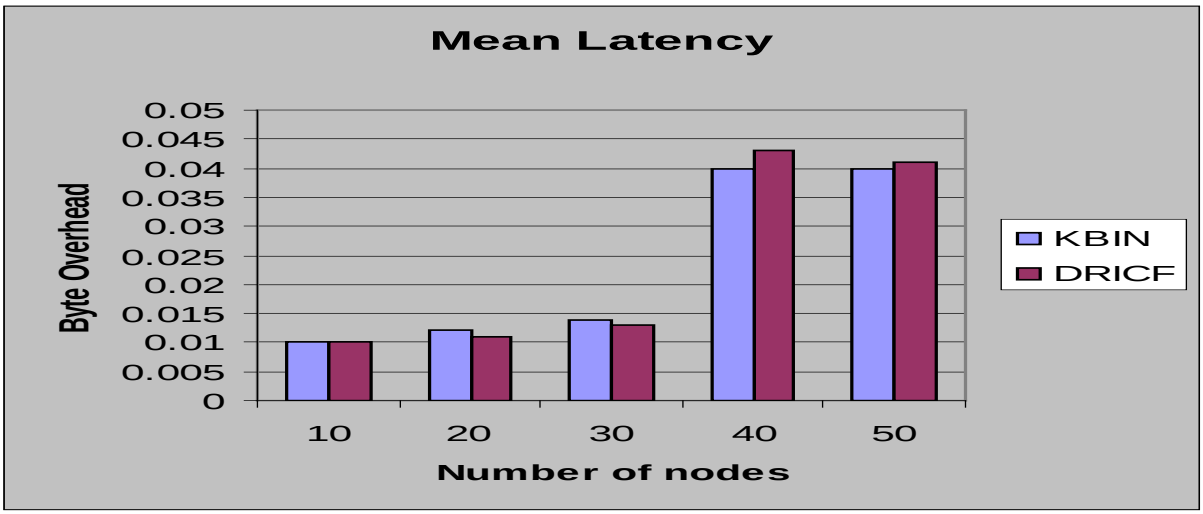

Fig. 7 Mean Latency among DRCIF and KBIN

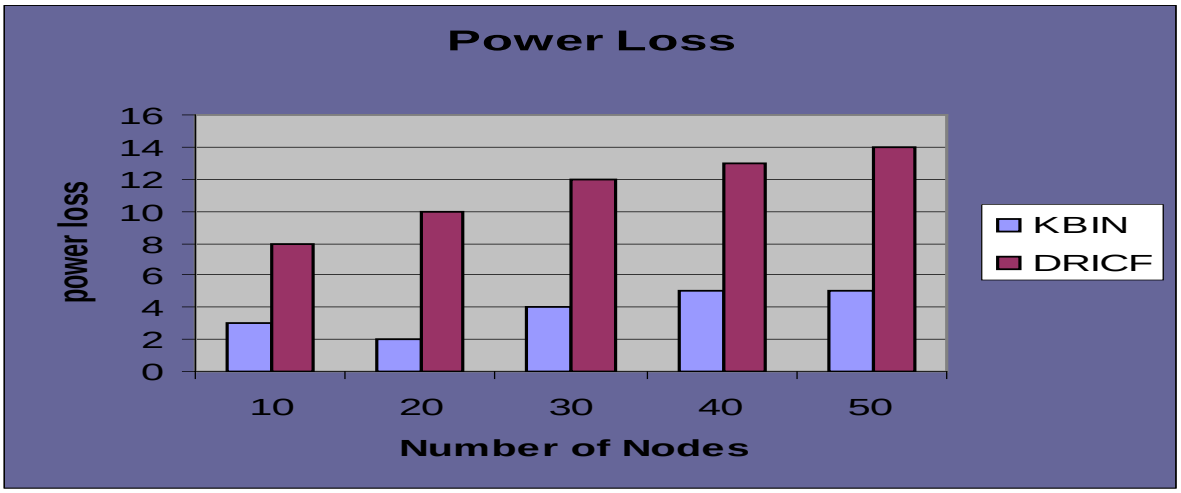

Fig. 8 Power Loss among DRCIF and KBIN

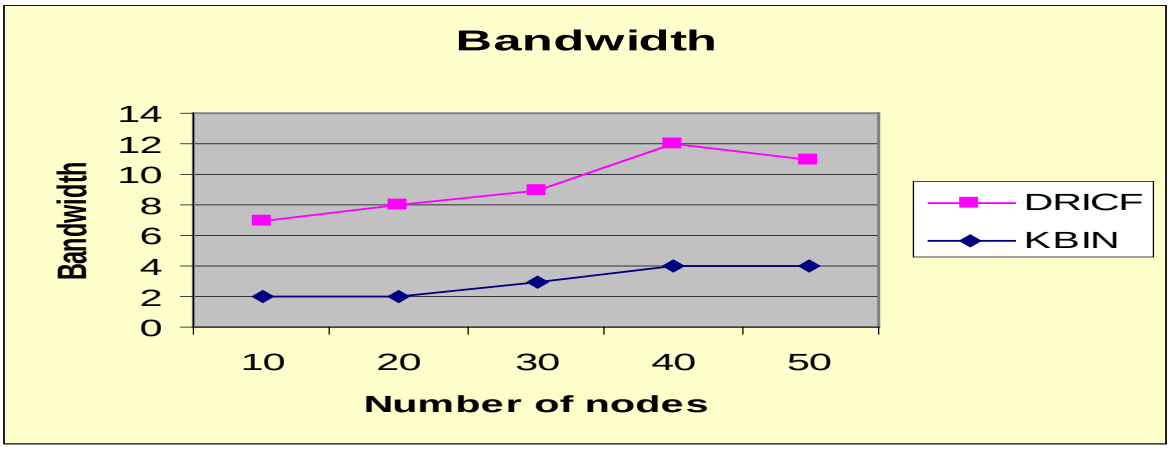

Fig. 9 Bandwidth among DRCIF and KBIN

VI. Conclusion

The proposed knowledge based intelligent node system mitigates the MANET routing attacks. Also investigated the performance and practicality of proposed approach based on several metrics and experiment results clearly demonstrated the effectiveness and scalability of proposed system. Routing attacks like route salvage attack, sleep deprivation attack and colluding miss relay attack are significantly reduced with the proposed approach. Moreover, a systematic way is developed to accommodate attack frequency and node reputation in proposed model.

References

[1] K. Liu, Y. Sun, W. Yu, Z. Han, Feb. 2006, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," .

[2] M. Eltoweissy, M. Refaei, L. DaSilva, May 2010, "Adaptation of Reputation Management Systems to Dynamic Network Conditions in Ad Hoc Networks".

[3] C. Keser, P. Cheng, P. Rohatgi and G. Wagner, 2007, "Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control".

[4] K. Levitt, M. Bishop and S. Wang, C. Tseng, 2007, "Cost-Sensitive Intrusion Responses for Mobile Ad Hoc Networks".

[5] Ziming Zhao and Gail-Joon Ahn, 2012, "Risk-Aware Mitigation for MANET Routing Attacks".

[6] P.Jacquet and T. Clausen, 2003, "Optimized Link State Routing Protocol" Network Working Group.

[7] C. Kruegel, 2002, "Evaluating the Impact of Automated Intrusion Response Mechanisms".

[8] J. Wong and C. Strasburg, N. Stakhanova, S. Basu, 2009,Intrusion Response Cost Assessment Methodology".

[9] Y. Zheng and L. Teo, G. Ahn, 2003, "Dynamic and Risk-Aware Network Access Management".

[10] D. Holmer, C. Nita-Rotaru, and B. Awerbuch, 2008, "ODSBR: An On-Demand Secure Byzantine Resilient Routing Protocol for Wireless Ad Hoc Networks".

[11] S. Wang and C. Ko, 2006, "DEMEM: Distributed Evidence-Driven Message Exchange Intrusion Detection Model for Manet," Proc and Recent Advances in Intrusion Detection".

[12] T. Song and K. Levitt, 2006, "A Specification-Based Intrusion Detection Model for OLSR," Proc. Ninth Int'l Symp. Recent Advances in Intrusion Detection (RAID".

[13] M. Debbabi and P. Bhattacharya, 2011, “Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET,” IEEE Trans. Dependable and Secure Computing.
[14] J. Felix, C. Joseph, and A. Das, 2011, “Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA,” IEEE Trans. Dependable and Secure Computing.
[15] S. Marti, M. Baker and T. Giuli, 2000, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” Proc. ACM MobiCom.
[16] S. Kurosawa, A. Jamalipour, H. Nakayama and N. Kato, 2006, “Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method,” Int’l J. Network Security.
[17] D. Johnson and Y. Hu, 2004, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks”.
[18] C. Kruegel and T. Toth, 2002, “Evaluating the Impact of Automated Intrusion Response Mechanisms,” Proc. 18th Ann. Computer Security Applications Conf.
[19] S. Basu, J. Wong and C. Strasburg, 2009, “Intrusion Response Cost Assessment Methodology,” Proc. Fourth ACM Symp, Information, Computer, and Comm. Security.
[20] L. Teo, G. Ahn, and Y. Zheng, 2003, “Dynamic and Risk-Aware Network Access Management,” Proc. Eighth ACM Symp