International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:12, 2014

Malicious Route Defending Reliable-Data Transmission Scheme for Multi Path Routing in Wireless Network

S. Raja Ratna, R. Ravi

***Abstract*—**Securing the confidential data transferred via wireless network remains a challenging problem. It is paramount to ensure that data are accessible only by the legitimate users rather than by the attackers. One of the most serious threats to organization is jamming, which disrupts the communication between any two pairs of nodes. Therefore, designing an attack-defending scheme without any packet loss in data transmission is an important challenge. In this paper, Dependence based Malicious Route Defending DMRD Scheme has been proposed in multi path routing environment to prevent jamming attack. The key idea is to defend the malicious route to ensure perspicuous transmission. This scheme develops a two layered architecture and it operates in two different steps. In the first step, possible routes are captured and their agent dependence values are marked using triple agents. In the second step, the dependence values are compared by performing comparator filtering to detect malicious route as well as to identify a reliable route for secured data transmission. By simulation studies, it is observed that the proposed scheme significantly identifies malicious route by attaining lower delay time and route discovery time; it also achieves higher throughput.

***Keywords*—** Attacker, Dependence, Jamming, Malicious.

I. Introduction

WIRELESS networks are highly exposed to jamming attack due to its openness of communication [4], [10], [22]. Due to jammer obstacle, the transmitted packets can be either blocked or modified or replaced, leading to deficient in national and personal security. Jamming interferences the communication between nodes and its objective is to prevent the legitimate sender or receiver from transmitting or receiving packets. One of the most powerful jammer is the reactive jammer which disrupts the packet by injecting unwanted error bits into it, thereby allowing the packet to reach the receiver side wrongly [8], [11]. As a result, jamming-resistant and identification of malicious route in which the jammer resides are very vital.

Different jamming models are studied and reactive jamming is found to be the smarter and power efficient model that targets only the reception of packet. The various jamming models [5], [9], [20] that are studied and dealt in this paper are constant, random, deceptive, selective [18], and reactive [3], [16], [21].

S. Raja Ratna is a full time Research Scholar with the Anna University recognized Research Center in Francis Xavier Engineering College, Tirunelveli, Tamil Nadu 627003 India (phone: 91 9486938282; fax: 0462-2501007; e-mail: gracelinrr@yahoo.com).

Dr. R. Ravi is a dean with the Computer Science and Engineering Research Department, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu 627003 India (e-mail: csehod@francisxavier.ac.in).

In this paper, Dependence based Malicious Route Defending DMRD Scheme has been proposed. The main steps of DMRD are route capturing, agent marking, comparator filtering, malicious route detection and reliable route identification. In agent dependence value marking, the dependence values for all the routes are marked using triple agents. In comparator malicious route filtering, the dependence values are compared by performing comparator filtering to detect the malicious route.

The paper proceeds as follows. Section II describes related works. Section III describes system model of the proposed work. Section IV explains the proposed scheme. The Section V presents the simulations conducted in order to evaluate the proposed scheme and summarizes the result. Finally, Section VI concludes the paper.

II. Related Works

The focus of this work is to detect the malicious route as well as to identify a reliable route. There are a number of prior works that aid in detecting it. Jamming attacks in wireless networks can be categorized into two, detection and prevention; both of them have been studied and developed using various defence schemes.

The challenges of employing multipath routing have been recognized, for example, Hossen et al. [7] proposes Availability History Vectors (AHV)-based algorithms for improving the jamming resilience in wireless network, it addresses the problem of selecting multiple route using MicaZ nodes based on the knowledge of route's previous history. The routes history are recorded and calculated through history vectors.

To minimize congestion and to achieve security via multipath routing, Zhang et al. [15] explained a load balancing scheme to distribute traffic along the selected multiple paths using multiple path routing protocol. In order to maximize packet delivery ratio, Aristotelis et al. [14] developed a theoretical routing model and coding scheme to evaluate multipath routing, that simultaneously splits the information across the given disjoint paths, so that the information is received without excessive delay.

Eric et al. [13] proposed an analytical congestion-optimized traffic partitioning model based on the global real-time traffic to minimize the network congestion in the network and compares it with load balancing heuristic.

Ying et al. [2] proposes an application-layer real-time trigger-identification service to defend reactive jammers. This scheme identifies all the trigger nodes, which invokes jammer

nodes during its transmission. However, the service overhead is higher.

Richa et al. [19] proposes a self-stabilizing distributed medium access control ANTIJAM protocol to mitigate internal reactive jammers with complete knowledge of the past history. But this work does not focus on physical layer jamming. Finally, Xu et al. in [17] have further extended [12] to consistently monitor jamming signals. A Prototype using MICA2 Mote platform has been designed to detect the presence of four different jamming attack models in wireless network.

The proposed scheme has four-fold contributions over prior schemes: 1) All routes in the path are checked individually to detect the malicious route. 2) It captures the benefit of filtering process using three comparators. 3) To identify a reliable route, instead of a single metric as in previous works, the proposed scheme uses three agent based dependence metrics. 4) By this scheme, jamming probability is reduced to a greater extent and the routes are categorized correctly using comparators.

III. System Model

A. Problem Statement

The wireless network consisting of random deployment of n cooperative simple reliable nodes are connected through wireless links. Consider two nodes u and v which communicate in a multi hop route with u being the source and v the sink. A jammer is placed within the nearness of one of the intermediate hops in the transmission path between u and v intensely listening to all the network activities. When u transmits a packet to v, the jammer in between them corrupts the packet by injecting high level of noise and then retransmits the jammed packet to the sink. The objective of this work is to detect malicious route in which the jammer resides and also to identify a reliable route for secured data transmission. The main scenario is to make the packet reach the receiver securely without jamming effect. The realization of jamming attack is shown in Fig. 1.

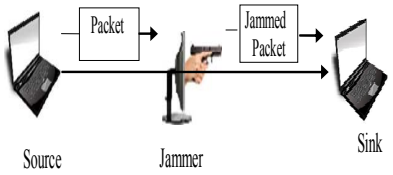

Fig. 1 Realization of jamming attack

B. Overview of Dependence based Malicious Route Defending Scheme

The proposed Dependence based Malicious Route Defending Scheme is a two layered architecture composing of two steps: a) Agent Dependence Value Marking Step and b) Comparator Malicious Route Filtering Step. These steps combine together to perform the functions such as dependence value calculation and malicious route identification. The outline system design architecture of DMRD scheme is shown in Fig. 2.

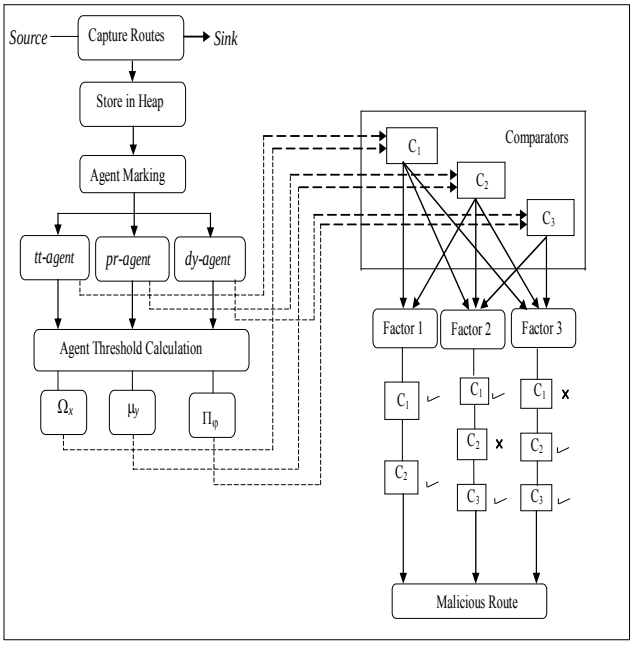

Fig. 2 Design architecture of DMRD Scheme

- The Agent Dependence Value Marking Step, captures all possible routes between the source and sink, it then calculates the dependence values for all the routes using triple agents and maintain it in the heap at the sink.
- In Comparator Malicious Route Filtering Step, the dependence values are compared by performing comparator filtering to detect malicious route as well as to identify reliable route.

IV. Dependence Based Malicious Route Defending DMRD Scheme

A. Initialization Process

The purpose of initialization process is to capture all possible routes between u and v with a jammer in between them. For m captured routes $CR=\{cr_j|j\in[1,m]\}$, the dependence values are calculated. To perform dependence comparison, the captured routes are maintained at the sink. The sink maintains a heap H_m which holds the forwarders list, forwarders id, number of hops, source node, the start time of the route, the end time, the total number of packets received, the total number of packets sent, the total number of packets dropped, the sequence number of packets and the protocol used information's for m routes.

B. Agent Dependence Value Marking Step

Dependence values are obtained using three agents, the throughput T_x denoted as *tt-agent*, delay d_x^{ly} denoted as *dy-agent* and packet delivery ratio P_x^{dr} denoted as *pr-agent*. The *tt-agent*, *dy-agent* and *pr-agent* are calculated for m routes in H_m, $\{(T_x, P_x^d, d_x^{ly})|x\in[1,m]\}$. The *tt-agent* [1, 6] is calculated

as in (1) where l is the number of blocks in the packet, c is the checksum length, f_r is the frame error rate which represent the probability that a packet cannot be correctly decoded and n, k are the error control codes being used.

$$T_X = \frac{(lk - c)(1 - f_r)}{nl} \tag{1}$$

The T_x mean value μ_k is calculated as in (2) and its threshold value is $\Omega_x=(\mu_k+(\mu_k/m))$.

$$\mu_k = \left(1/m\right) \sum_{x=1}^{m} T_x \tag{2}$$

The *pr-agent* P_x^{dr} is a good candidate to detect jamming and it can also be lowered because of congestions or failures. Studies in [17] show that even in a highly congested situation where the traffic rate is 19.38 kb/s with maximum bandwidth capacity of 12.364 kb/s at 100 percent duty cycle, the P_x^{dr} measured by the receiver is still around 78 percent. The *pr-agent's* threshold can be used to differentiate jamming from network congestion. In this paper, the jammer node is considered closer to the sink and the packet size is kept small, so that the source can send out the packet reliably. If the jammer interrupts transmission, then the receiver could not receive the packets correctly, thus the P_x^{dr} value is lowered as in [5], [12]. If the source sends N_S packets and if only N_R packets are successfully received, then P_x^{dr} is denoted as in (3).

$$P_x^{dr} = \frac{N_R}{N_S} = \frac{\text{Number of packets successfully received by receiver}}{\text{Number of packets send out by sender}} \tag{3}$$

The P_x^{dr} mean value μ_y for m routes is given by (4) and its *pr-agent* threshold is $\mu_y=(\gamma_{pdr}+(\gamma_{pdr}/m))$.

$$\gamma_{pdr} = \left(1/m\right) \sum_{x=1}^{m} P_x^{dr} \tag{4}$$

The third agent used for measuring jamming is *dy-agent* d_x^{ly} and it gets increased by the presence of jammer. If the packet transmission time under jamming *t[jam]* exceeds the normal packet transmission time *t[pkt],* then d_x^{ly} occurs. Since the packet size is kept small, the jammer cannot jam within *t[pkt]*. To find d_x^{ly} in transmitting the packet from the source to the sink, the number of routers R_u^v, the transmission delay ∂_{tr}, propagation delay ∂_{pg} and processing delay ∂_{pr} are measured. The *dy-agent* is calculated using (5) where l_p denotes the packet length, r_t the transmission rate, d_{uv} the distance between the source and sink, and $\varepsilon_r(\omega)$ the relative permittivity.

$$\partial_x^{ly} = \left(R_u^v + 1\right)\left[\partial_{tr} + \partial_{pg} + \partial_{pr}\right] \Rightarrow \left(R_u^v + 1\right)\left[\frac{l_p}{r_t} + \frac{d_{uv}}{1/\sqrt{\varepsilon_r(\omega)}} + \partial_{pr}\right] \tag{5}$$

The *dy-agent* for m routes in H_m is $\{(d_x^{ly})|x\in[1,m]\}$. The d_x^{ly} mean ∂_n is given in (6) and its threshold is $\Pi_\varphi= (\partial_n-(\partial_n/m))$.

$$\partial_n = \left(1/m\right) \sum_{x=1}^{m} \partial_x^{ly} \tag{6}$$

C. Comparator Malicious Route Filtering Step

The values Ω_x, μ_y and Π_φ obtained from T_x, P_x^{dr} and d_x^{ly} act as the filtering mechanism. The calculated *tt-agent* T_x, *pr-agent* P_x^{dr} and *dy-agent* d_x^{ly} for m routes in H_m is compared with the calculated Ω_x, μ_y, Π_φ values, this comparison is done using three comparators C_1, C_2 and C_3. The comparator C_1 compares whether T_x is less than or equal to Ω_x, C_2 compares whether P_x^{dr} is less than or equal to μ_y and C_3 compares whether d_x^{ly} is greater than or equal to Π_φ, represented as $C_1 \leftarrow(T_x\leq\Omega_x)$, $C_2\leftarrow(P_x^{dr}\leq\mu_y)$, $C_3 \leftarrow(d_x^{ly}\geq\Pi_\varphi)$. The three decision factor's dealing with C_1, C_2 and C_3 are σ_1, σ_2 and σ_3. Decisive factor 1 deal with C_1 and C_2, whereas decision factor 2 and 3 deals with C_1, C_2 and C_3.

Decision factor 1 (σ_1): If a route's C_1 and C_2 conditions are satisfied, then that route is placed in the set $J^1{}_C$, whereas if both conditions are not satisfied it is placed in the set $T^1{}_R$. If C_1 condition is satisfied, whereas C_2 condition is not satisfied, then the route is checked with decision factor 2. If C_2 is satisfied and C_1 is not satisfied, it is checked with decision factor 3. The decision factor 1 is explained in (7).

$$\sigma_1 \Rightarrow (C_1, C_2) \rightarrow \begin{cases} J_C^1 & \text{if } \left\{\left(T_x \leq \Omega_x\right) \wedge \left(P_x^{dr} \leq \mu_y\right)\right\} \\ T_R^1 & \text{if } \left\{\left(T_x > \Omega_x\right) \wedge \left(P_x^{dr} > \mu_y\right)\right\} \end{cases} \tag{7}$$

Decision factor 2 (σ_2): If C_1condition is satisfied, whereas C_2 condition is not satisfied, then this strategy is dealt by decision factor 2. In σ_2, the comparator C_3 is used to decide whether to place the route in $T^2{}_R$ or $J^2{}_C$ as explained in (8). If C_3condition is satisfied, then the route is placed in $J^2{}_C$ else in $T^2{}_R$.

$$\sigma_2 \Rightarrow (C_1, C_2, C_3) \rightarrow \begin{cases} J_C^2 & \text{if} \left\{(T_X \leq \Omega_X) \wedge \left(P_x^{dr} > \mu_y\right) \wedge \left(d_x^{ly} \geq \Pi_\varphi\right)\right\} \\ T_R^2 & \text{if} \left\{(T_X \leq \Omega_X) \wedge \left(P_x^{dr} > \mu_y\right) \wedge \left(d_x^{ly} < \Pi_\varphi\right)\right\} \end{cases} \tag{8}$$

Decision factor 3 (σ_3): If C_1 condition is not satisfied, whereas C_2 is satisfied this strategy is dealt by decision factor 3. In σ_3, C_3 decision becomes important, if C_3 condition is satisfied, then the route is placed in $J^3{}_C$ else in $T^3{}_R$ as in (9).

$$\sigma_3 \Rightarrow (C_1, C_2, C_3) \rightarrow \begin{cases} J_C^3 & \text{if} \left\{(T_X > \Omega_X) \wedge \left(P_x^{dr} \leq \mu_y\right) \wedge \left(d_x^{ly} \geq \Pi_\varphi\right)\right\} \\ T_R^3 & \text{if} \left\{(T_X > \Omega_X) \wedge \left(P_x^{dr} \leq \mu_y\right) \wedge \left(d_x^{ly} < \Pi_\varphi\right)\right\} \end{cases} \tag{9}$$

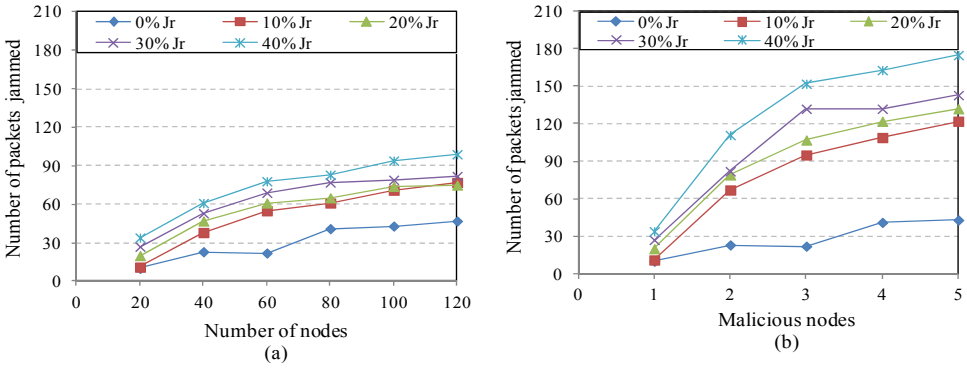

Fig. 3 Number of packets jammed for different jamming ratios (a) Network size (b) Malicious nodes

The sets J^1_C, J^2_C, J^3_C of σ_1, σ_2 and σ_3 contains misbehaviouring routes, whereas T^1_R, T^2_R, T^3_R contains normal routes. The routes of J_C and T_R are put together in two separate sets *Mis-rou* and *Nor-rou* respectively, where *Mis-rou*=$\{J^1_C, J^2_C, J^3_C\}$ stands for misbehaving route and *Nor-rou*=$\{T^1_R, T^2_R, T^3_R\}$ for normal route. The filtering process carried out by C_1, C_2 and C_3 is shown in (10), if the comparators conditions are satisfied it is denoted as '=1', else as '≠1'.

$$Mis-rou \Leftarrow \begin{cases} (C_1=1),\ (C_2=1) \\ (C_1=1),\ (C_2\neq 1),\ (C_3=1) \\ (C_1\neq 1),\ (C_2=1),(C_3=1) \end{cases}$$

$$Nor-rou \Leftarrow \begin{cases} (C_1\neq 1),(C_2\neq 1) \\ (C_1=1),(C_2\neq 1),(C_3\neq 1) \\ (C_1\neq 1),\ (C_2=1),(C_3\neq 1) \end{cases} \quad (10)$$

Algorithm 1: Comparator Filtering Step

1. **for** all $cr_j \in CR | j \in [1,m]$ **do**
2. calculate *tt-agent*, *pr-agent*, *dy-agent*
3. obtain Ω_x, μ_y and Π_φ from agents
4. *Filtering Process:*
5. **if** $((T_x \leq \Omega_x)$ and $(P_x^{dr} \leq \mu_y))$ **then**
6. place $cr_j \rightarrow J^1_C$
7. **else if** $((T_x \leq \Omega_x)$ and $(P_x^{dr} > \mu_y)$ and $(d_x^{ly} \geq \Pi_\varphi))$ **then**
8. place $cr_j \rightarrow J^2_C$
9. **else if** $((T_x > \Omega_x)$ and $(P_x^{dr} \leq \mu_y)$ and $(d_x^{ly} \geq \Pi_\varphi))$ **then**
10. place $cr_j \rightarrow J^3_C$
11. **else**
12. place $cr_j \rightarrow T_R$
13. **end if**
14. record $\{J^1_C, J^2_C, J^3_C\} \Rightarrow$ *Mis-rou*
15. record $\{T^1_R, T^2_R, T^3_R\} \Rightarrow$ *Nor-rou*
16. **end for**
17. identify reliable route from *Nor-rou*
18. reliable route $\leftarrow ((T_x > \Omega_x)$ and $(P_x^{dr} > \mu_y)$ and $(d_x^{ly} < \Pi_\varphi))$

The routes in *Mis-rou* are ranked based on its number of occurrences in the set and they are indexed in descending order. The route with the highest number of occurrence in the set is the malicious route. Packets are not transmitted in the identified malicious route, and a reliable route is identified for secure data transmission. A route in *Nor-rou* is identified as reliable when its three comparator conditions are not satisfied $\{C_1 \neq 1, C_2 \neq 1, C_3 \neq 1\}$ or $\{(T_x > \Omega_x), (P_x^{dr} > \mu_y), (d_x^{ly} < \Pi_\varphi)\}$. After identifying the reliable route between *u* and *v*, the packets are transmitted in that route. The algorithm for comparator filtering step is explained in Algorithm 1.

V. Performance Evaluation

The experimental results of the proposed System are presented in this section. With the aid of ns-2, the effectiveness and efficiency of the proposed system is evaluated under no congestion environment. Simulation is run on a 500 x 500 m^2 network with a random topology of 100 nodes using AODV protocol. Clients and server exchange by communicating 2 KB size of data using TCP protocol with 128 bytes of data per packet. The network performance is measured by throughput, delay time, route discovery time and number of packets jammed.

A. Simulation on Packets Jammed for Varying Percentage of Jamming

In the first set of experiment, the number of packets jammed is studied for increasing jamming ratio. The jamming ratio Jr is a measure of how jamming will happen, and it is the value between 0 (0% jamming) and 100 (100% jamming). Higher the ratio, more will the jamming be. From Figs. 3 (a) and (b), it is observed that the number of packets jammed has significant impact on the network size and the number of malicious nodes. As jamming ratio and malicious node count increases, the number of packets jammed also increases.

B. Simulation of Packet Size on Delay Time

In the second set of experiment, the delay time is studied as a function of increasing packet size. Fig. 4 shows the simulation results of no jamming NOJ, the DMRD scheme, and for five different jamming models constant, random deceptive, selective and reactive. The proposed scheme is studied under both congestion and no congestion environment. As the packet size increases, the delay time also increases. The queuing delay due to congestion provides extra time for packet transmission when compared to no congestion packet

transmission. Therefore, congestion delay time of DMRD is smaller than no congested delay time.

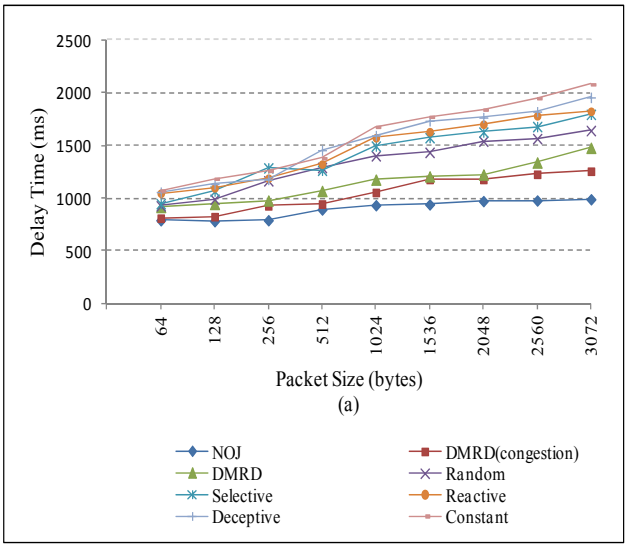

Fig. 4 Delay Time for jamming models

C. Simulation of Route Discovery Time for Different Jamming Models

In the third set of experiment, the route discovery time is studied for different jamming models as a function of increasing packet size. Fig. 5 shows that, as the packet size increases, the time required for identifying the route also increases. Extra time incurred due to queuing delay in congestion provides lesser route discovery time when compared to no congestion route discovery time. Therefore, congestion route discovery time of DMRD is smaller than no congested route discovery time.

D. Simulation of Average Throughput for Different Percentage of Jamming

In the fourth set of experiment, average throughput is studied for different jamming models under no congestion environment. Table I shows the simulation results for NOJ, DMRD using reactive jammer under congestion and no congestion, reactive, deceptive, random and constant. As the jamming ratio increases, the throughput decreases and the DMRD's throughput under congestion is higher than no congestion throughput.

E. Simulation on DMRD Scheme

In the fifth set of experiments, average throughput is simulated under four observations: i) No Attack ii) DMRD with congestion iii) DMRD without congestion and iv) No Defence. Fig. 6 (a) shows the throughput for increasing number of network nodes with a single jammer in the transmission path. Fig. 6 (b) is simulated as a function of increasing malicious nodes. As the number of malicious nodes increase, the throughput decreases. DMRD congestion throughput is higher when compared to no defense and no congestion throughput.

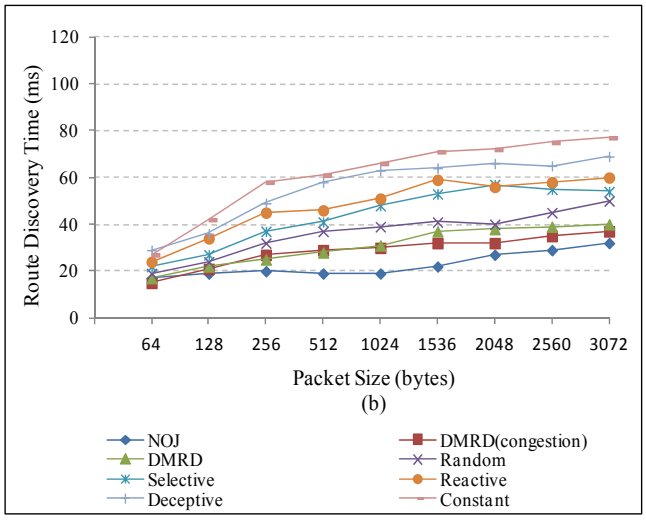

Fig. 5 Route Discovery Time for different jamming models

TABLE I
AVERAGE THROUGHPUT FOR VARYING JAMMING RATIO

Jamming Models	Average Throughput (Mbps)				
	0% Jr	10% Jr	20% Jr	30% Jr	40% Jr
NOJ	0.175	0.175	0.175	0.175	0.175
DMRD (congestion)	0.175	0.169	0.165	0.155	0.148
DMRD	0.175	0.158	0.152	0.140	0.131
Reactive	0.175	0.134	0.139	0.129	0.121
Deceptive	0.175	0.135	0.132	0.124	0.117
Random	0.175	0.127	0.122	0.120	0.111
Constant	0.175	0.121	0.101	0.98	0.89

VI. CONCLUSION

The paper addresses the problem of prevention of jamming attack with the goal of defending malicious route in multi path routing environment. In this paper, Dependency based Malicious Route Defending scheme has been proposed based on agent dependency values. The key idea is to select possible routes between pair of nodes in which the jammer resides and the captured paths are recorded in the heap at the sink. In order to defend malicious route, the agent dependent values are compared using comparator filtering and a reliable route is identified for secure transmission. The network performance of the proposed scheme has been examined both under congestion and no congestion in terms of average throughput, delay time and route discovery time. The efficiency of the scheme is well supported by simulation and various sophisticated attack models are simulated under different network settings. Simulation result shows that the proposed scheme under congestion yields better performance when compared to no congestion; it also limits the distorting ability of the jammer. One leftover problem is the identification of jammer node which can be analysed in the future work.

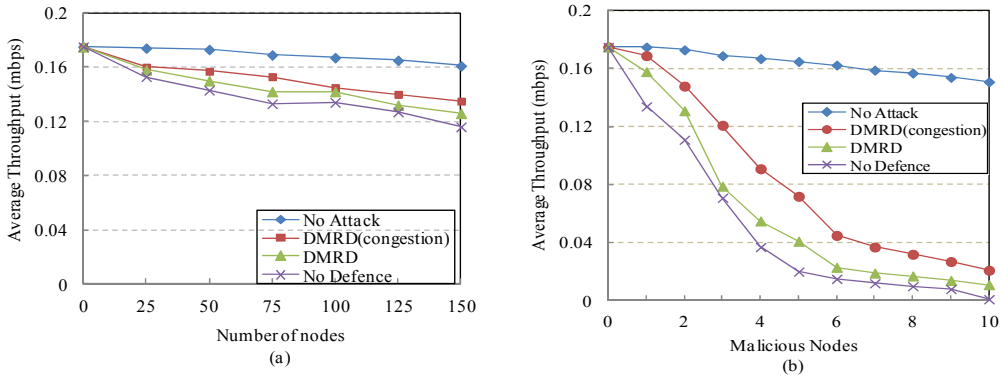

Fig. 6 Average Throughput for the proposed scheme (a) Network size (b) Malicious nodes

ACKNOWLEDGEMENT

This work was supported in part by Anna University recognized research center lab at Francis Xavier Engineering College, Tirunelveli, India.

REFERENCES

[1] G. Lin, and G. Noubir, "On link layer denial of service in data wireless LANs", *Wireless Communications and Mobile Computing*, vol. 5, pp. 273–284, May 2004.

[2] Y. Xuan, Y. Shen, N. P. Nguyen, and M. T. Thai, "A trigger identification service for defending reactive jammers in WSN", *IEEE Transactions on Mobile Computing*, vol. 11, pp. 793 – 806, May 2012

[3] H. Nguyen, T. Pongthawornkamol, and K. Nahrstedt, "Alibi framework for identifying reactive jamming nodes in wireless lan", *IEEE Globecom Telecommunication Conference*, pp. 1-6, Dec. 2011.

[4] C. Li, H. Dai, L. Xiao, and P. Ning, "Communication efficiency of anti-jamming broadcast in large-scale multi-channel wireless networks", *IEEE Transactions on Signal Processing*, vol. 60, pp. 5281 - 5292 Oct. 2012.

[5] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: the case of jammers", *IEEE Communications surveys & tutorials*, vol. 13, pg. 245-257, May 2011.

[6] G. Noubir, and G. Lin, "Low-power DoS attacks in data wireless lans and countermeasures", *Mobile Computing and Communications Review*, vol. 7, pp. 29–30, July 2003.

[7] H. Mustafa, X. Zhang, Z. Liu, W. Xu, and A. Perrig, "Jamming-resilient multipath routing", *IEEE Transactions on Dependable and Secure Computing*, vol. 9, pp. 852-864, Nov. 2012.

[8] S. R. Ratna, R. Ravi, and B. Shekhar, "An Intelligent Approach based on Neuro- Fuzzy Detachment Scheme for Preventing jamming Attack in Wireless Networks", *Journal of Intelligent and fuzzy logic*, Doi 10.3233/IFS-141363. ISSN 1064-1246(Print). 1875-8967 Online (in press), Sep. 2014.

[9] Y. S. Shiu, S. Y. Chang, H.C. Wu, S.C.H. Huang, and H. H. Chen, "Physical layer security in wireless networks: a tutorial", *IEEE Wireless Communications*, vol. 18, pp. 66-74, April 2011.

[10] Q. Peng, P. C. Cosman, and L. B. Milstein, "Spoofing or Jamming: Performance Analysis of a Tactical Cognitive Radio Adversary", *IEEE Journal of selected areas in communications*, vol. 29, pp. 903-911, April 2011.

[11] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "On the performance of IEEE 802.11 under jamming", *Proc. IEEE* Conference on Computer Communications *INFOCOM*, pp 1265–1273, Apr. 2008.

[12] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming Sensor Networks: Attack and Defense Strategies", *IEEE Networks Special Issue on Sensor Networks*, vol.20, pp. 41-47, May 2006.

[13] E. Setton, X. Zhu, and B. Girod, "Congestion-Optimized Multi-Path Streaming of Video over Ad Hoc Wireless Networks," *Proc. IEEE Int'l Conf. Multimedia and Expo (ICME)*, vol. 3, pp. 1619 – 1622, June 2004.

[14] A. Tsirigos, and Z. J. Haas, "Analysis of Multipath Routing part I: The Effect on the Packet Delivery Ratio," *Proc. IEEE Trans. Wireless Comm.*, vol. 3, pp. 136-146, Jan. 2004.

[15] L. Zhang, Z. Zhao, Y. Shu, and Lei Wang, "Load Balancing of Multipath Source Routing in Ad Hoc Networks," Proc. IEEE International Conference on Communications, vol. 5, pp. 3197 – 3201, 2002.

[16] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders,"Reactive jamming in wireless networks: How realistic is the threat?", *In Proceedings of WiSec*, pp. 47-52, 2011.

[17] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", *MobiHoc 05*, pp. 46-57, May 2005.

[18] A. Proano, and L. Lazos," Packet-Hiding Methods for Preventing Selective Jamming Attacks", *IEEE Transactions on dependable and secure computing*, vol. 9, pp. 101 - 114, Jan. 2012.

[19] A. Richa, C. Scheideler, S. Schmid, and J. Zhang,"An Efficient and Fair MAC Protocol Robust to Reactive Interference", *IEEE/ACM Transactions on Networking*, vol. 21, pp. 760 - 771, June 2013.

[20] L. Wang, and A. M. Wyglinski, "A Combined Approach for Distinguishing Different Types of Jamming Attacks against Wireless Networks", *IEEE Pacific Rim (PacRim) Conference on Communications, Computers and Signal Processing*, pp. 8019-814, Aug. 2011.

[21] H. Nguyen, T. Pongthawornkamol, and K. Nahrstedt,"Alibi framework for identifying reactive jamming nodes in wireless LAN", *IEEE Global Telecommunication Conference (GLOBECOM 2011)*, pp. 1-6, Dec. 2011.

[22] K. Pelechrinis, M. Iliofotou, and S. Krishnamurthy, "A measurement – Driven Anti-jamming System for 802.11 Networks", *IEEE/ ACM Transactions on Networking*, vol. 19, pp. 1208-1222, Aug. 2011.

S. Raja Ratna received her B.E degree in Electrical and Electronics Engineering from The Indian Engineering College, Tirunelveli in 2000, and the M. Tech degree in Computer and Information Technology from Manonmanium Sundaranar University, Tirunelveli in 2005. She is working towards Ph. D degree at the Information and Communication Engineering at Anna University, Chennai. Her research interests include denial-of-service attacks, jamming attacks, secure routing algorithm and security in networks.

Dr. R. Ravi is an Editor in International Journal of Security and its Applications (South Korea). He is presently working as a Professor & Head and Research Centre Head, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli. He completed his B.E in Computer Science and Engineering from Thiagarajar College of engineering, Madurai in the year 1994 and M.E in Computer Science and Engineering from Jadavpur Government research University, Kolkatta. He has completed his Ph. D in Networks from Anna University Chennai. He has 19 years of experience in teaching as Professor and Head of department in various colleges. He published 25 International Journals. He is also a full time recognized guide for various Universities. Currently he is guiding 18 research scholars. His areas of interest are Virtual Private networks, Networks, Natural Language Processing and Cyber security.