Trust Based Suspicious Route Categorization for Wireless Networks and its Applications to Physical Layer Attack

S. RAJA RATNA[1], DR. R. RAVI [2]
[1]Research Scholar, Department of Computer Science and Engineering,
Francis Xavier Engineering College, Tirunelveli, INDIA
[2]Professer and Head, Department of Computer Science and Engineering,
Francis Xavier Engineering College, Tirunelveli, INDIA
[1]gracelinrr@yahoo.com, [2]csehod@francisxavier.ac.in

Abstract: - With the increased usage of networks, security becomes a significant issue. Owing to the open nature, the adversary corrupts the packet by injecting high level of noise, thereby keeping the channel busy so that legitimate traffic gets completely blocked resulting in packet loss at the receiver side. Although several schemes have been proposed to prevent these attacks but none of the existing works have analyzed trust based routing. Nowadays trust based routing is an effective way to prevent the physical layer attacks in wireless network. In this paper, prevention of physical layer attack has been studied by comparing trust metrics. A new scheme known as Trust based Suspicious Route Categorization (TSRC) has been proposed which identifies the misbehaving suspicious routes and it operates in two modules. In module one, the misbehaving routes are marked as suspicious based on its trust condition. In module two, the marked suspicious routes are categorized into four groups using a classifier and from the no risk group a reliable route is selected for data transmission. By simulation studies, it is observed that the proposed scheme significantly identifies suspicious routes with higher detection rate and lower false positive probability; it also achieves higher throughput and lower delay.

Key-words: - Categorization, Delay, Misbehaving, Physical layer, Suspicious, Throughput.

1. Introduction

A wireless network is a collection of wireless nodes connected through wireless links with the nodes communicating directly or through multiple hops. Data is sent between nodes by hopping through intermediate nodes. Due to the open and distributed nature, the wireless networks are highly vulnerable to various malicious activities [1], [2]. Anyone with a transceiver can eavesdrop on wireless transmission or jam legitimate ones. Eavesdropping can be prevented using cryptographic methods, where as jamming attack is hard to detect. The jammer [3] involving in malicious activity either continuously emits signal on the channel by disrupting the communication, or it will overpower transmitted signal by injecting high level of noise [4], [5]. It is important to protect the data from this attack and allow the data to reach the receiver side safely. Traditional security solutions are often inadequate, therefore to improve security of data and to prevent the data being attacked; one idea is to identify a reliable route based on trust metrics. To facilitate the implementation of this idea various trust metrics which quantify trust relationships have been considered and integrated into routing metric.

Jammers are of four models constant, random, deceptive and reactive. The constant jammer constantly injects random sequence of bits, while the deceptive jammer is also similar to constant jammer but constantly injects continuous sequence of bits. Power inefficiency is the main drawback of the two jammers. The random jammer is power efficient because it randomly jams. The smarter and power efficient is the reactive jammer [6] targeting only the reception of packet and deterministically jam only when the communication medium is busy.

The attacker use little energy to prevent the receiver from receiving legitimate packet, thereby degrading throughput [7], packet delivery ratio and increasing delay. Throughput, Packet Delivery Ratio and Delay are good

candidates against jamming. Throughput is the rate of successful data delivered over a communication channel in a given amount of time and it degrades because of jamming. Packet delivery ratio can be lowered because of congestion or failures. Studies in [8] shows 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 packet delivery ratio measured by the receiver is still around 78 percent. The packet delivery ratio lowered for jamming is much higher than due to network congestion. Delay increases, as the jamming time exceeds the packet transmission time.

In this paper, we propose Trust based Suspicious Route Categorization (TSRC) Scheme to select a reliable route to prevent jamming attack. The main steps of TSRC are trust based route marking, suspicious route categorization and reliable route identification. In trust based route marking, the misbehaving routes are marked as suspicious based on its trust condition. In suspicious route categorization, the suspicious routes are categorized into groups and then the reliable route identification selects a reliable route for secure data transmission.

The paper proceeds as follows. Section 2 describes related works. Section 3 describes system model of the proposed work. Section 4 explains the proposed scheme. The Section 5 presents the simulations conducted in order to evaluate the proposed scheme and summarizes the result. Finally, Section 6 concludes the paper.

2. Related Works

To the best of our knowledge, there is no previous work that helps to prevent jamming attack using trace metrics. In the recent literature, a plentiful of general approaches has been proposed on prevention of jamming attack. We reviewed related works on detection of jamming attacks, jammers characteristics, and prevention of jammers on different types of jamming attacks.

Proano *et. al.* in [9] have investigated the impact of an internal selective jammer who targets packets of high importance. The adversary is active only for a short period. They have also explained selective jamming in terms of network performance degradation. They have developed three schemes that prevent real time packet classification by combining cryptographic primitives with physical layer attributes. The packets to be transmitted are hidden between physical and MAC layer and then transmitted. Throughput and delay are studied on different types of jammers.

Chiang *et. al.* in [10] have proposed an optimized power efficient code tree system that provides input to physical layer and also helps the physical layer circumvent the jammer. Each receiver cooperates with the transmitter to detect any jamming that affects the receiver. Each transmission is sent on at most 2j+1 code simultaneously and results are based on evaluating packet delivery ratio.

Richa *et. al.*[11] have proposed a simple, fair, self-stabilizing distributed MAC protocol called ANTIJAM to mitigate internal interference, requiring no knowledge about the number of participants in the network and it is also robust to intentional and unintentional external interference. The protocol is efficient and fair against powerful reactive adversaries who have complete knowledge of the past history. ANTIJAM features low convergence time and has excellent fairness property and also achieves constant throughput. Throughput is dealt under different jamming strategy as a function of network size.

Li *et. al.* [12] have evaluated the communication efficiency of Uncoordinated FH (UFH) and Collaborative UFH (CUFH) in large-scale networks with the aim of preventing jamming in multi-channel networks using network delay as a metric. In this network the numbers of nodes are large and may exceed the number of channels. Without the use of secret keys, UFH achieves robustness to inside jammers but achieves poor communication efficiency due to the lack of coordination between the source and sink. Sub-optimal protocol CUTH-p has been proposed which simplifies the implementation of CUFH. In order to obtain better packet reception rate the number of relays are controlled in CUFH.

Pelechrinis *et. al.* [13] have investigated an Anti-jamming Reinforcement System for random jammers and it uses both power control and rate control module to prevent jamming. Based on channel condition, the rate adaptation module assigns the transmission rate. In order to increase successful packet reception, power control module tunes the clear channel assessment threshold. Appropriate tuning allows the transmitter to send packets even when jammed and it is examined using throughput as a metric.

Pelechrinis *et. al.* [14] have proposed proactive frequency hopping technique to prevent jamming attack. A game theoretic approach is used to capture the interaction between link and jammer employing frequency hopping. If the number of orthogonal channel was larger, then proactive FH would be very effective in terms of throughput.

Popper *et. al.* in [15] focused on spread-spectrum anti-jamming broadcast without the requirement of shared secrets. The uncoordinated direct sequence spread spectrum modulation scheme is used by the communication nodes.

Chen *et. al.* [16] proposed a trust management protocol in Delay tolerant networks to detect attackers. The author combines QOS trust with social trust to obtain a composite trust metric. However this protocol cannot be demonstrated for real time applications.

Finally, Bao *et. al.* [17] proposed a cluster-based hierarchical trust management protocol for wireless sensor networks to deal with malicious nodes. The author demonstrated the feasibility of dynamic hierarchical trust management using trust-based IDS applications. But implementing this complex scheme at every member in a cluster is very complicated.

The proposed scheme has five-fold contribution over prior schemes 1) all routes are checked individually to identify suspicious 2) It captures the benefit of trust based system, and performs both route marking and categorization using trust values to detect suspicious route, rather than just only node as in prior works. 3) To provide a reliable route for data transmission, instead of single trust metric as in previous works, the proposed scheme uses three trust metrics. 4) This scheme reduces jamming probability to great extent 5) To enhance network performance, the routes are correctly categorized using a classifier 5) It accurately predicts suspicious routes at higher detection rate and lower false probability.

3. System Model

3.1 Problem Statement

Consider two nodes *u* and *v* which communicate through wireless medium with *u* being the source and *v* the sink. A jammer is present within the communication range of *u* and *v* intensely listening all the network activities. When the node *u* transmits a packet to node *v*, the jammer which is in between them corrupts the packet by injecting high level of noise (extra bits). The objective of the proposed scheme is to prevent the jammer from injecting unwanted bits into the packet, thereby allowing the packet to reach the receiver side safely. Prevention of jamming attack is not feasible without the detection of jammer in the suspicious route.

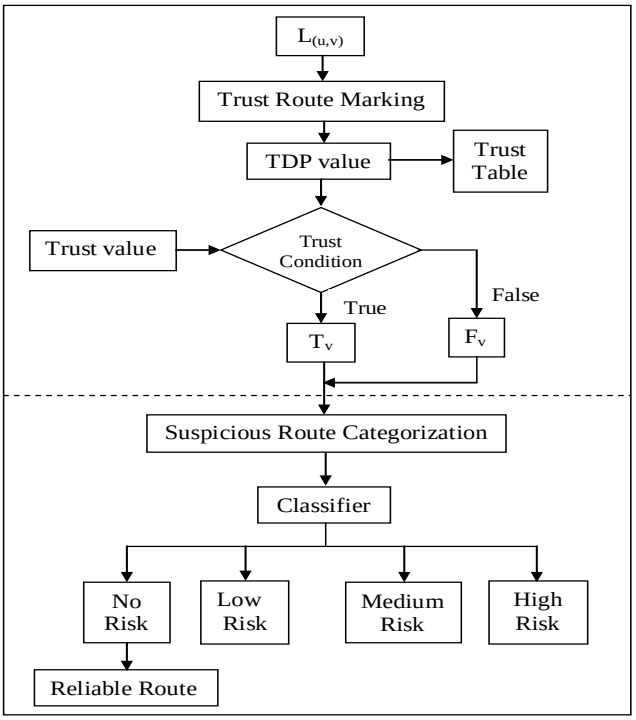

Figure 1. System Design of TSRC scheme

Upon identification of suspicious route they are categorized and a reliable route is identified for

data transmission. The main scenario is to make the network free from jammers, thereby lowering the jamming effect and also improve network performance.

3.2 Overview of Trust Based Suspicious Route Categorization Scheme

The proposed Trust Based Suspicious Route Categorization Scheme is the integration of two techniques: a) Trust based Route Marking and b) Categorization of Suspicious Route. These techniques combine together to perform the functions such as identification of suspicious routes between the source and the sink and categorizing them. The outline system design of TSRC scheme is shown in Figure 1.

- The Trust based Route Marking technique, finds all possible routes to reach the sink, it then calculates the *TDP* values for all the routes and maintain it in the trust table at the sink. Using the trust condition, the misbehaving routes are marked as suspicious.
- In Categorization of Suspicious Route technique, the marked suspicious routes are categorized into four groups and then from the no risk group a reliable route is selected for data transmission.

4. Trust based Suspicious Route Categorization (TRSC)

4.1 Initialization Process

Consider two nodes u and v which communicate through wireless medium with u being the source and v the sink. A jammer J is present within the communication range of u and v intensely listening all the network activities. Before the source u transmits a packet to the sink v, the source finds out m possible routes to reach the sink. The sink maintains a log file $L_{(u,v)}$ for m routes between u and v. The log file contains sets $Q_j<v>$ for all m routes $RT= \{rt_j \mid j \in [1, m]\}$ having list of variables such as source id u_{id}, number of forwarders f_k , list of forwarders ($f_1, f_2 \ldots. f_n$), number of packets send N_{PS} , number of packets successfully received N_{PR} and sink node id v_{id}. Let S_N be the sequence number of each packet with $S_N \in (1, N_{PS})$. Start time S_{time} and end time E_{time} represents the sending time and receiving time of the packet. The set at the sink is represented as follows:

$$\sum_{j=1}^{m} Q_j<v> = \begin{bmatrix} u_{id},\ f_k,\ \{f_1, f_2 \ldots. f_n\},\ N_{PS}, \\ N_{PR}, \langle S_{time}, S_N \rangle,\ \langle E_{time}, S_N \rangle,\ v_{id} \end{bmatrix}$$

In order to precede trust comparison, n rounds $RD= \{rd_i \mid i \in [1, n]\}$ are needed for m routes with a total of n x m routes. The sink calculates *TDP* values, the throughput denoted as *T-value* τ, the delay denoted as *D-value* ∂ and packet delivery ratio denoted as *P-value* ρ for n x m routes. The sink maintains a table with rounds as rows and routes as columns, and the calculated *TDP* values are placed in the table. Calculate TDP values for n x m routes and store it in the set $d_{(r,t)}$ as shown in equation (1).

$$d_{(r,t)} = \sum_{i=1}^{n} \sum_{j=1}^{m} \left[\tau_{ij}, \partial_{ij}, \rho_{ij} \right] \quad (1)$$

4.2 Trust based Route Marking

The *T-value* τ, the *D-value* ∂ and *P-value* ρ in the table for n x m routes is compared with its threshold trust values α, β and γ. If the trust comparison condition given in equation (2) is satisfied, represent it by a true value T_v else by a false value F_v. If τ greater than or equal to α it is T_v, similarly if ∂ is lesser than or equal to β it is T_v, likewise if ρ is greater than or equal to γ it is T_v, else it is F_v.

$$Trust\,Condition: \begin{cases} T_V \leftarrow \{(\tau \geq \alpha) \| (\partial \leq \beta) \| (\rho \geq \gamma)\} \\ F_V \leftarrow \{(\tau < \alpha) \| (\partial > \beta) \| (\rho < \gamma)\} \end{cases} \quad (2)$$

A sample model of the trust comparison for n x m traces is represented as a table format with routes as rows and rounds as column. The three *TDP* values are represented as *U(x)*. Let $\tau_{(1)}$ be the *T-value* for round1, similarly $\tau_{(2)}$ is the *T-value* for round 2. The trust comparison model is shown in Table 1.

After all routes have been marked with F_v or T_v, either of the following patterns is obtained for each route as illustrated below:

- $\{T_v\ T_v\ T_v\}$: All the *TDP* values are marked as T_v.
- $\{T_v\ T_v\ F_v\}$: Two *TDP* values are marked with T_v, while remaining one is marked as F_v.

Table 1. Trust value comparison

R	rd_1			rd_2			…	rd_n		
$U(x)$	$u_1(x)$	$u_2(x)$	$u_3(x)$	$u_1(x)$	$u_2(x)$	$u_3(x)$	…	$u_1(x)$	$u_2(x)$	$u_3(x)$
	$\tau_{(1)}$	$\partial_{(1)}$	$\rho_{(1)}$	$\tau_{(2)}$	$\partial_{(2)}$	$\rho_{(2)}$	…	$\tau_{(n)}$	$\partial_{(n)}$	$\rho_{(n)}$
rt_1	T_v	F_v	T_v	F_v	F_v	F_v		T_v	T_v	T_v
rt_2	F_v	T_v	F_v	F_v	T_v	T_v		T_v	F_v	F_v
rt_3	F_v	F_v	F_v	T_v	T_v	T_v		T_v	T_v	T_v
:							…			
rt_m	T_v	T_v	T_v	T_v	T_v	F_v		F_v	T_v	F_v

- $\{F_v\, F_v\, T_v\}$: One *TDP* value is marked as T_v, while the remaining two factors are marked as F_v.
- $\{F_v\, F_v\, F_v\}$: All the *TDP* values are marked as F_v.

Based on the above cases, traces are categorized using suspicious route categorization algorithm.

4.3 Categorization of Suspicious Route Algorithm

This section categorizes the routes in $d_{(r,t)}$ using Suspected Trace Categorization algorithm. The route data is predicted and categorized into four groups: i) *no risk* group ii) *low risk* group iii) *medium risk* group and iv) *high risk* group based on naive Bayesian classifier [18]. Let *n* x *m* be the list of route data and each data tuple is represented by the set of attributes, $U(x) = \{u_1(x), u_2(x)\ldots.. u_r(x)\}$. Table 1 shows the sample route data model. The *n* x *m* routes in route data model is predicted and placed in *i* number of groups which is depicted as $G_i = \{G_1, G_2\ldots\ldots G_r\}$. Let G_1 corresponds to *no risk* group, G_2 corresponds to *low risk* group, G_3 corresponds to *medium risk* group and G_4 corresponds to *high risk* group.

Based on highest posterior probability, the classifier predicts that the given data tuple $U(x)$, belongs to the groups G_i. The route data has three attributes namely *T-value, D-value* and *P-value.* For example, consider a data tuple $U(x)$ depicted as $U(x)$ = (*T-value* $=T_v$, *D-value*$= F_v$, *P-value*$= T_v$). The attributes t-factor and p-factor are satisfied by its trust, while d-factor is not satisfied; the classifier predicts the tuple and places it in group G_2. By equation (3) the classifier maximizes the probability that the tuple $U(x)$ belongs to the groups G_i if and only if

$$P\left(G_i \mid U(x)\right) > P\left(G_j \mid U(x)\right) \quad \forall\ j \in \left\{1, m\right\},\ i \neq j \qquad (3)$$

$P(G_i|U(x))$ is the probability of G_i conditioned on $U(x)$. Initially the classifier calculates the probability that each trace belongs to any one kind of groups *no risk* group, *medium risk* group, *low risk* group and *high risk* group. $P(U(x)|G_i)$ is the probability of $U(x)$ conditioned on G_i and $P(G_i)$ is the probability of G_i. The traces are categorized as in equation (4).

$$P(G_i \mid U(x)) = \frac{P(U(x) \mid G_i) \times P(G_i)}{P(U(x))} \qquad (4)$$

$$P(U(x) \mid G_i) = \sum_{y=1}^{r} P\left(u_y(x) \mid G_i\right)$$

$$= P\left(u_1(x) \mid G_i\right) \times P\left(u_2(x) \mid G_i\right) \times \ldots. \times P\left(u_r(x) \mid G_i\right) \qquad (5)$$

The probabilities of $P(u_1(x)|G_i)$ x $P(u_2(x)|G_i)$ x ……..x $P(u_r(x)|G_i)$ in equation (5) are estimated from the data tuple of $U(x)$. After categorization, routes in G_1 have zero probability to have jammer in it, low probability for G_2, medium probability for G_3 and high probability for G_4 groups.

Let's discuss four groups:

Case 1: *no risk* group (G_1) In this case all the three *TDP* values gets satisfied by their trust. The routes in G_1 have zero probability to have jammer in it. These types of routes are placed in *no risk* group.

Case 2: *low risk* group (G_2) Either of these possibilities occurs $\{T_v\, T_v\, F_v\}$ or $\{T_v\, F_v\, T_v\}$ or $\{F_v\, T_v\, T_v\}$ here. In this case two *TDP* values get

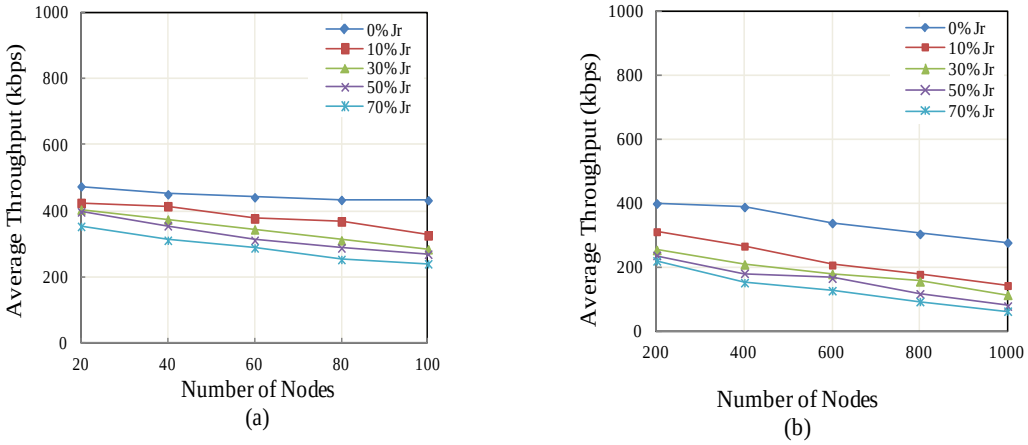

Figure 2. Average Throughput for increasing Jamming Ratio (a) Smaller Network (b) Larger Network

satisfied with its trust, while remaining one does not gets satisfied. Hence it has only one F_v and two T_v. The route with low probability to have jammer in it is placed in *low risk* group.

Case 3: *medium risk* group (G_3) In this case, there are three possibilities {T_v F_v F_v} or {F_v F_v T_v} or {F_v T_v F_v}. Here only one *TDP* value gets satisfied with its trust, while remaining two does not. So it has only one T_v and two F_v. The route with medium probability to have jammer in it is placed in *medium risk* group.

Case 4: *high risk* group (G_4) In the last case, all the *TDP* values are not satisfied with their trust, the *T-value* is less than its trust, while *D-value* is greater than its trust and *P-value* is lesser than its trust. Therefore the route has three F_v and no T_v, the possibility to have jammer in it is high and it is placed in *high risk* group.

The routes in *no risk* group (G_1) have zero probability to have jammer in it and the routes in it are reliable. A route is chosen from G_1 for data transmission, while the routes in other groups are marked as suspicious and the packets are not transmitted in that route. By this process data can be safely transmitted and jamming also can be prevented.

Categorization of Suspected Route is explained in algorithm1.

Algorithm 1: Categorization of Suspected Routes

for all $rd_i \in RD$ **do**
  for all $rt_j \in RT$ **do**
    calculate $d_{(r,t)}$
    if (t_j ($U(x)$) > trust) **then**
      $u_i(x) := Tv$
    else
      $u_i(x) := Fv$
    categorize t_j to $G_i \mid i \in [1,4]$
    if ($P\left(G_i \mid U(x)\right) > P\left(G_j \mid U(x)\right)$) **then**
      $P(G_i \mid U(x)) = \frac{P(U(x) \mid G_i) \times P(G_i)}{P(U(x))}$
      place $t_j \rightarrow G_i$
  $P\left(J_i^G\right)$ ={null, low, medium, high}|$i \in [1,4]$

5. Experimental Evaluation

A network of 500 x 500 m^2 is used for simulation with a random topology of 100 nodes. Network performance is measured by throughput, packet delivery ratio and delay. A 2 Kb file is transferred between the source and the sink connected via multiple hops in a wireless network.

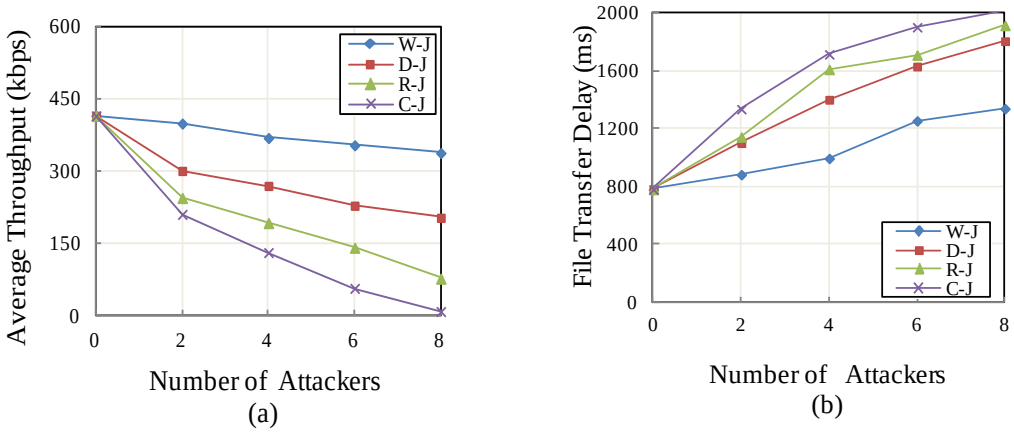

Figure 3. Experimental Results with increasing Number of Attackers for Different Types of Jammers (a) Average Throughput (b) File Transfer Delay

5.1 The Impact of Increasing Network Size for Different Jamming Ratio

The first set of experiments, simulate average throughput as a function of increasing network size. The figures show the network performance under 5 different jamming ratio (Jr) observations for both smaller network and larger networks. From Figure 2a and b it is observed that, as the network size increases the throughput degrades for larger network but slightly degrades for smaller network. Jamming ratio (Jr) is a measure or estimation of how likely jamming will happen. It is the value between 0 (0% chance for jamming to occur) and 100 (100% chance for jamming to occur). Higher the degree of ratio, more likely the jamming will happen. In case of no jammer (0% Jr) for larger network, the throughput degrades by 278kbps for 1000 nodes and 339 for 600 nodes, while throughput degrades from 451kbps to 433kbps for 20 nodes to 100 nodes because of normal packet loss. Second, with 10% Jr and third with 30% Jr with single jammer, the throughput degrades when compared to no jammer because of jamming activity. Fourth, with 50% Jr and fifth with 70% Jr with single jammer, throughput again degrades as shown (238kbps for 200 nodes, 80kbps for 1000 nodes with 50% Jr and 221kbps for 200nodes, 64kbps for 1000nodes with 70% Jr). From the above it is observed that as the network size and jamming ratio increases, throughput decreases.

5.2 The Impact of Increasing Number of Attackers for Different Types of Jammers

The Second set of experiments, simulate average throughput and file transfer delay *E[d]* as a function of number of attacker nodes. It is compared for Without Jamming *W-J*, Randomly Jamming *R-J*, Constantly Jamming *C-J* and Deterministically Jamming *D-J* using reactive jammers. Throughput decreases and delay increases under jamming effect. Figure 3a and b shows the simulation results under 4 different criteria's. The first criteria in the case of without jammer, throughput slightly decreases while delay slightly increases due to normal loss and it has no effect on the number of attackers. Second with *D-J*, throughput decreases when compared to *W-J* but higher than *C-J* and *R-J* because *D-J* does not degrade a lot like other jammers because it deterministically jam only when the communication medium is busy. Third with *R-J*, throughput degrades by 245kbps for two malicious nodes and 193kbps for 4 malicious nodes, while delay increases to 1143ms for 2 malicious nodes and 1609ms for 4 malicious nodes. Fourth with *C-J*, throughput greatly degrades while delay increases a lot because this jammer continuously jams the network (211kbps, 1335ms for 2 attacker nodes and 132kbps, 1713ms for 4 attacker nodes). As the number of attacker nodes increases, the network performance is greatly affected. Since reactive

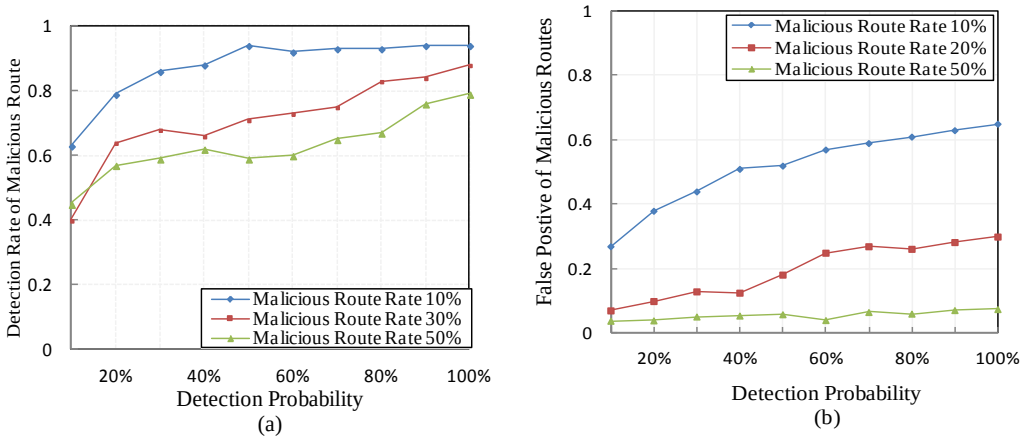

Figure 4. Experimental Results with increasing detection probability for different malicious route rate (a) Detection Rate (b) False Positive of Malicious Routes

jammers are powerful its performance does not degrade like *R-J* and *C-J*.

Table 2 shows packet delivery ratio (PDR) for different jamming ratio (Jr). If Jr increases, packet delivery ratio decreases for increasing number of jammers (N_{jam}). The PDR degrades a lot for multiple jammers when compared to single jammer. PDR becomes very low when the number of jammer exceeds four.

Table 2. PDR (%) for different Jr

Jr	N_{jam}			
	2	4	6	8
20%	45	22	12	9
40%	37	20	10	6
60%	32	17	7	2
80%	28	13	3	0
100%	24	9	0	0

5.3 The Impact of Increasing Detection Probability with TSRC

In the third set of experiment, Figure 4a and b shows the detection rate and false positive probability of malicious routes for three different malicious route rates (10%, 30% and 50%). From the said figure, it is observed that a route with 50% malicious route rate can be easily detected by TSRC at a lower detection rate and lower false positive probability. The route with 50% malicious rate provides better detection probability at lower detection rate, while detection rate is pretty higher for 10% and 30% malicious rates. Likewise is the false positive probability, a route with 50% malicious route rate provides better detection probability at very low false positive probability, while false positive is higher for 10% and 30% malicious rates.

5.4 The Impact of Choosing Different *T-Trust* values

In the fourth set of experiment, Figure 5 shows the percentage of routes in four different groups (No Risk Group G_1, Low Risk Group G_2, Medium Risk Group G_3 and High Risk Group G_4) for different *T-Trust* value. From the said figure, it is observed that for lower *T-Trust* value nearly 80% of the routes are placed in G_1 group and only 15% of the routes are placed in G_4.

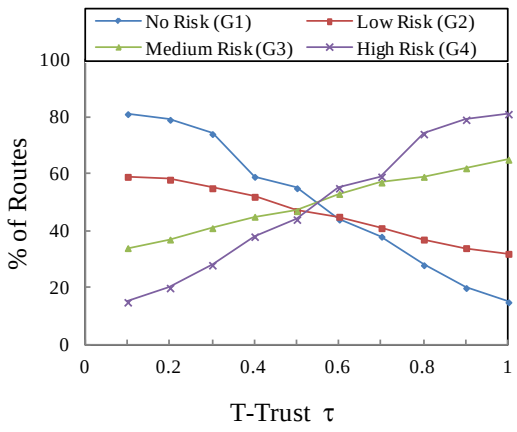

Figure 5. Experimental Results with increasing T-Trust against percentage of routes in different groups

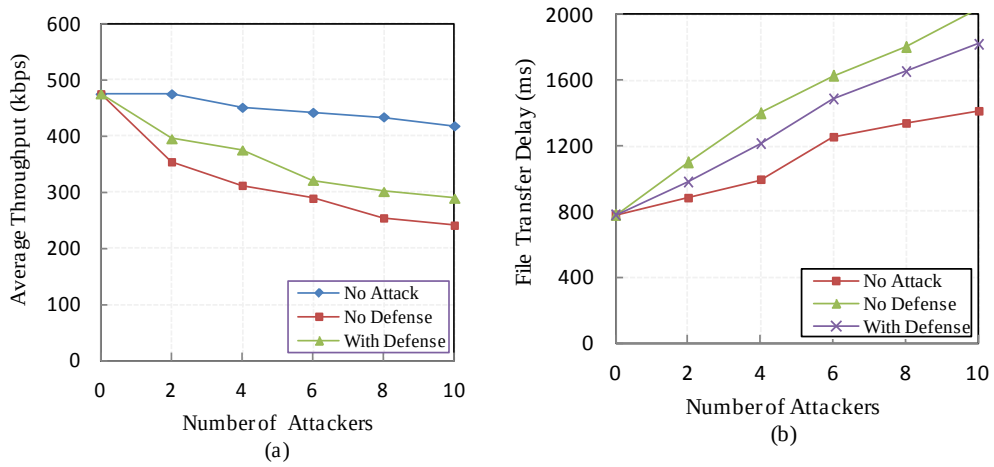

Figure 6. Experimental Results with increasing Number of Attackers for different schemes (a) Average Throughput (b) File Transfer Delay

Whereas for higher *T-Trust* values majority of the routes are placed in G_4 and very lower amount of the routes are placed in G_1. The routes in groups G_2 and G_3 does not differs like G_1 and G_4, but the number of routes in group G_2 decreases for increasing *T-Trust* and number of routes in group G_3 increases for increasing *T-Trust* values.

5.5 The Impact of Proposed Scheme for Increasing Number of Attackers

In the fifth set of experiment, Figure 6a and b represents the simulation of average throughput and delay under three observations i) No Attack ii) No Defense and iii) With Defense using TSRC Scheme. They are simulated as a function of increasing number of attacker nodes. The throughput increases for With Defense criteria when compared to No Defense criteria, but as the number of attacker node increases With Defense slightly decreases. With defense criteria provide lower delay than no defense criteria but higher than no attack criteria. The TSRC scheme provides higher throughput and lower delay even if the number of attacker nodes increases. Thus with TSRC scheme malicious routes are better identified and discriminated, thereby lowering jamming effect.

Table 3 shows Packet Delivery Ratio (PDR) for increasing number of jammers (N_{jam}) under three criteria's, No Attack (NA), No Defense (ND) and With Defense (WD) using TSRC scheme. If the number of jammers (N_{jam}) increases, packet delivery ratio decreases. It is very low for ND criteria; by using the proposed scheme PDR value is higher in WD when compared to ND but lower than NA. PDR becomes very low for increasing number of jammers.

Table 3. PDR (%) for three Criteria

N_{jam}	NA	ND	WD
2	75	45	62
4	73	22	51
6	71	12	36
8	69	9	27

The proposed scheme helps to prevent the jammer from attacking the financial servers of the corporate sectors so that the servers could respond to the legitimate clients. The experimental setup works well for smaller network but the performance slightly degrades when the network size increases. The limitation of the proposed scheme is that it relays on the previous history log files, therefore it suffers from additional overhead due to log file maintenance and also trust values has to be correctly calculated and maintained at the table.

These limitations can be analysed and rectified in the next work.

6. Conclusion

This paper proposes an effective Trust based Suspicious Route Categorization (TSRC) Scheme for preventing physical layer jamming attack. The attacker is considered as a part of the network and corrupts the packets by injecting extra bits into it. It is experimentally verified that reactive jammers is more vulnerable and is severe than other jammers by means of its throughput and file transfer delay. The proposed scheme first marks the misbehaving route based on its trust value and then categorize the marked suspicious route to select a reliable route for data transmission. Suspicious routes are categorized into four groups using a classifier and then a reliable route is identified from no risk group for successful data transmission. The simulation result shows that TSRC scheme yields better throughput of 395kbps and lower delay of 981ms for 2 jammers and it also limits the distorting ability of the jammer. It is experimentally verified that TSRC scheme provides better detection rate and lower false positive probability. The proposed scheme helps to prevent the jammer from attacking the financial servers of the corporate sectors so that the servers could respond to the legitimate clients. Additional overhead due to trust value calculation for each trace can be focussed in the future research work.

Acknowledgement

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

References

[1] P. Yi, Y. Wu, F. Zou, and N. Liu,"A Survey on Security in Wireless Mesh Networks", *IETE Technical Review*, Vol. 27, No. 1, pp. 6-14, 2010.

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

[3] D. M. Shila, Y. Cheng and T. Anjali, "Mitigating selective forwarding attacks with a channel-aware approach in WMNs", *IEEE transactions on wireless communications*, vol. 9, no.5, pp. 1661-1675, May 2010.

[4] M. Furdek and N. S. Kapov, "Attack-Survivable Routing and Wavelength Assignment for high-power jamming", *17th International Conference Optical Network Design and Modeling (ONDM)*, 2013, pp. 70 - 75.

[5] H. Nguyen, T. Pongthawornkamol, and K. Nahrstedt, "Alibi framework for identifying reactive jamming nodes in wireless LAN", *IEEE Globecom 2011 proceedings*, 2011, pp. 1-6.

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

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

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

[9] A. Proano, and L. Lazos," Packet-Hiding Methods for Preventing Selective Jamming Attacks", *IEEE Transactions on dependable and secure computing*, Vol. 9, No. 1, January/February 2012.

[10] Jerry T. Chiang and Yih-Chun Hu, "Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks", *IEEE/ACM Transactions on Networking*, Vol. 19, No. 1, February 2011.

[11] 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, No. 3, pp. 760 - 771, June 2013.

[12] 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, No. 10, October 2012.

[13] Pelechrinis K., IIiofotou M., and Krishnamurthy S., “A measurement – Driven Anti-jamming System for 802.11 Networks”, *IEEE/ ACM Transactions on Networking*, Vol .19, No.4, pp. 1208-1222, 2011.

[14] K. Pelechrinis, C. Koufogiannakis, and S. V. Krishnamurthy, “On the Efficacy of Frequency Hopping in Coping with Jamming Attacks in 802.11 Networks”, *IEEE Transactions on wireless communications*, Vol. 9, No. 10, October 2010.

[15] C. Popper, M. Strasser, and S. Capkun, “Jamming - Resistant Broadcast Communication without Shared Keys,” *Proc. USENIX Security Symp.*, 2009.

[16] I. R. Chen, F. Bao, M. J. Chang and J. H. Cho, “Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing”, *IEEE Transaction on Parallel and Distributed Systems*, Vol. 25, No.5, May 2014, pp.1200-1210.

[17] F. Bao, I. R. Chen, M. J. Chang and J. H. Cho, “Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection”, *IEEE transactions on network and service management*, Vol. 9, No.2, June 2012, pp.169-183.

[18] Jaiwei Han and Micheline Kamber, “Data Mining Concepts and Techniques”, Second Edition, *Morgan Kaufmann Publisher*, 2006.