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 interferes 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].

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.

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.

- 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 \( CR = \{ cr_j \mid j \in [1, m] \} \), 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 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 \( T_s \) denoted as \( tt-agent \), delay \( d_t^{by} \) denoted as \( dy-agent \) and packet delivery ratio \( P_d^{by} \) denoted as \( pr-agent \). The \( tt-agent \), \( dy-agent \) and \( pr-agent \) are calculated for \( m \) routes in \( H_m \), \( \{ (T_s, P_d^{by}, d_t^{by}) \mid x \in [1, m] \} \). 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, \( f_c \) 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.

\[
T_x = \frac{(k - c)(1 - f_c)}{nl}
\]

(1)

The \( T_x \) mean value \( \mu_k \) is calculated as in (2) and its threshold value is \( \Omega_{\mu} \cdot (\mu_k/m) \).

\[
\mu_k = \left( \frac{1}{m} \right) \sum_{x=1}^{m} T_x
\]

(2)

The \( pr\)-agent \( P_s^{dr} \) 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 \( P_s^{dr} \) 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 \( P_s^{dr} \) value is lowered as in [5], [12]. If the source sends \( N_k \) packets and if only \( N_k \) packets are successfully received, then \( P_s^{dr} \) is denoted as in (3).

\[
P_s^{dr} = \frac{N_k}{N_S} 
\]

(3)

The \( P_s^{dr} \) mean value for \( m \) routes is given by (4) and its \( pr\)-agent threshold is \( \mu_k \cdot (\gamma_{pd}^{dr} \cdot \gamma_{pd}^{tr} / m) \).

\[
\gamma_{pd}^{dr} = \left( \frac{1}{m} \right) \sum_{x=1}^{m} P_s^{dr}
\]

(4)

The third agent used for measuring jamming is \( dy\)-agent \( d_{by} \) 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 \( d_{by} \) occurs. Since the packet size is kept small, the jammer cannot jam within \( t[pkt] \). To find \( d_{by} \) in transmitting the packet from the source to the sink, the number of routers \( R_n \), the transmission delay \( \tilde{\tau}_v \), propagation delay \( \tilde{\tau}_g \), and processing delay \( \tilde{\tau}_p \) are measured. The \( dy\)-agent is calculated using (5) where \( \tau_p \) denotes the packet length, \( r \) the transmission rate, \( d_{cy} \) the distance between the source and sink, and \( \epsilon_{l}(\omega) \) the relative permittivity.

\[
\frac{d_{by}^{x}}{x} = \left( R_n + 1 \right) \left[ \tilde{\tau}_v + \tilde{\tau}_g + \tilde{\tau}_p \right] = \left( R_n + 1 \right) \frac{\tau_p}{\sqrt{\epsilon_{l}(\omega)}} + \frac{d_{by}^{x}}{\sqrt{\epsilon_{l}(\omega)}}
\]

(5)

The \( dy\)-agent for \( m \) routes in \( H_m \) is \( \{d_{by}^{x}(x)\} \in [1, m] \}. 

The \( d_{by} \) mean \( \tilde{\eta} \) is given in (6) and its threshold is \( \Pi_{\tilde{\eta}} \cdot (\tilde{\eta} / \omega) \).

\[
\tilde{\eta} = \left( \frac{1}{m} \right) \sum_{x=1}^{m} d_{by}^{x}
\]

(6)

C. Comparator Malicious Route Filtering Step

The values \( \Omega_{\mu}, \mu \) and \( \pi \) obtained from \( T_x, P_s^{dr} \) and \( d_{by} \) act as the filtering mechanism. The calculated \( tt\)-agent \( T_s \), \( pr\)-agent \( P_s^{dr} \) and \( dy\)-agent \( d_{by} \) for \( m \) routes in \( H_m \) is compared with the calculated \( \Omega_{\mu}, \mu, \pi \) values, this comparison is done using three comparators \( C_1, C_2 \) and \( C_3 \). The comparator \( C_1 \) compares whether \( T_s \) is less than or equal to \( \Omega_{\mu} \), \( C_2 \) compares whether \( P_s^{dr} \) is less than or equal to \( \mu \) and \( C_3 \) compares whether \( d_{by} \) is greater than or equal to \( \pi \). The three decision factor’s dealing with \( C_1, C_2 \) and \( C_3 \) are \( \sigma_1, \sigma_2, \sigma_3 \). 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 \((\sigma_1)\): If a route’s \( C_1 \) and \( C_2 \) conditions are satisfied, then that route is placed in the set \( T^1_R \), whereas if both conditions are not satisfied it is placed in the set \( T^2_R \). 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).

\[
\sigma_1 \Rightarrow \begin{cases} 
C_1, C_2 \rightarrow \begin{cases} 
T^1_R \quad \text{if } \left( T_s < \Omega_{\mu}, \left( P_s^{dr} < \mu \right) \right) \\
T^2_R \quad \text{if } \left( T_s > \Omega_{\mu}, \left( P_s^{dr} < \mu \right) \right)
\end{cases}
\end{cases}
\]

(7)

Decision factor 2 \((\sigma_2)\): If \( C_1 \) condition is satisfied, whereas \( C_2 \) condition is not satisfied, then this strategy is dealt by decision factor 2. In \( \sigma_2 \), the comparator \( C_3 \) is used to decide whether to place the route in \( T^2_R \) or \( J_C \) as explained in (8). If \( C_2 \) condition is satisfied, then the route is placed in \( J_C \) else in \( T^2_R \).

\[
\sigma_2 \Rightarrow \begin{cases} 
C_1, C_2, C_3 \rightarrow \begin{cases} 
T^1_C \quad \text{if } \left( T_s < \Omega_{\mu}, \left( P_s^{dr} > \mu \right) \right), \left( d_{by} \geq \pi \right) \\
T^2_R \quad \text{if } \left( T_s < \Omega_{\mu}, \left( P_s^{dr} > \mu \right) \right), \left( d_{by} < \pi \right)
\end{cases}
\end{cases}
\]

(8)

Decision factor 3 \((\sigma_3)\): If \( C_1 \) condition is not satisfied, whereas \( C_2 \) is satisfied this strategy is dealt by decision factor 3. In \( \sigma_3 \), \( C_3 \) becomes important, if \( C_3 \) condition is satisfied, then the route is placed in \( J_C \) else in \( T^2_R \) as in (9).

\[
\sigma_3 \Rightarrow \begin{cases} 
C_1, C_2, C_3 \rightarrow \begin{cases} 
T^1_C \quad \text{if } \left( T_s < \Omega_{\mu}, \left( P_s^{dr} > \mu \right) \right), \left( d_{by} < \pi \right) \\
T^2_R \quad \text{if } \left( T_s > \Omega_{\mu}, \left( P_s^{dr} > \mu \right) \right), \left( d_{by} < \pi \right)
\end{cases}
\end{cases}
\]

(9)
The sets $J^1_C$, $J^2_C$, $J^3_C$ of $\sigma_1$, $\sigma_2$ and $\sigma_3$ contains misbehavioring 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’.

$$
\begin{align*}
\text{Mis - rou} & = \{(C_1 = 1), (C_2 = 1)\} \\
\text{Nor - rou} & = \{(C_1 = 1), (C_2 = 1), (C_3 = 1)\}
\end{align*}
$$

**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 $\Omega_1$, $\mu_1$, and $\Pi_1$ from agents
4. Filtering Process:
5. if ($T_i \leq \Omega_2$ and ($P_i^\mu_1 \leq \mu_1$)) then
6. place $cr_j \rightarrow J^1_C$
7. else if ($T_i \leq \Omega_2$ and ($P_i^\mu_1 > \mu_1$) and ($d_i < \Pi_1$)) then
8. place $cr_j \rightarrow J^2_C$
9. else if ($T_i > \Omega_2$) and ($P_i^\mu_1 > \mu_1$) and ($d_i < \Pi_1$)) then
10. place $cr_j \rightarrow J^3_C$
11. else
12. place $cr_j \rightarrow T_R$
13. end if
14. record($J^1_C \cup J^2_C \cup J^3_C$) $\Rightarrow$ Mis-rou
15. record($T^1_R \cup T^2_R \cup T^3_R$) $\Rightarrow$ Nor-rou
16. end for
17. identify reliable route from Nor-rou
18. reliable route $\leftrightarrow$ ($T_i > \Omega_2$ and ($P_i^{\mu_1} > \mu_1$) and ($d_i < \Pi_1$))

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.

**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.

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.

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.
ACKNOWLEDGEMENT

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

REFERENCES


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 Thiahagarajar College of engineering, Madurai in the year 1994 and M.E in Computer Science and Engineering from Jadavpur Government research University, Kolkata. 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.