Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks

Kwangsung Ju and Kwangsue Chung

Department of Communications Engineering
Kwangwoon University, Seoul, Korea
ksju@cclab.kw.ac.kr, kchung@kw.ac.kr

Abstract

In a tactical field, wireless communication is prevailed among military agents and vehicles, but it is fragile by jamming attack from an adversary because of the wireless shared medium. Jamming attack is easily achieved by emitting continuous radio signal and it can interfere with other radio communications within the network. Channel switching over multiple channels or route detouring have been proposed to restore communication from jamming attacks, but they require a special radio system or knowledge of network topology. In this paper, in order to overcome limitations of the previous research, we propose a new robust rate adaptation scheme that is resilient to jamming attack in a wireless multi-hop tactical network. The proposed rate adaptation scheme detects jamming attack and selects the data transmission mode which has the expected maximum throughput based on the successful transmission probability. Through the performance evaluations, we prove rate adaptation scheme that improves packet delivery ratio and the wireless link utilization.

Keywords: *Tactical networks, Jamming attack, Rate adaptation, Multi-hop networks*

1. Introduction

C In tactical environments where no infrastructure exists, a wireless MANET (Mobile Ad hoc Network) attracts attention since military agents and vehicles must establish a self-organized network to exchange message that supports tactical operations. However, radio communications in the tactical MANET face several formidable security and reliability challenges due to the shared medium. One challenge is jamming [1].

A jamming attack is easily delivered by emitting continuous signal or injecting dummy packets into the shared medium causing interference with existing communications or in some cases abusing the MAC (Medium Access Control) layer of other nodes within a range. Consequently, jamming attack can seriously impede wireless communications. Previous jamming attack solutions showed that using spatial or spectrum diversity to cope with the jamming attack [2-5]. If nodes find the jamming attack, they switch communication channel [4] or send packets on a detour [2]. However, channel switching or detouring jamming area requires a special radio system or knowledge of the network topology. Moreover, these schemes do not utilize the jammed channels, though they have enough bandwidth for the data transmission.

In this paper, we propose a new robust rate adaptation scheme that is resilient to jamming attack in a wireless multi-hop tactical network. It improves the wireless link utilization by detecting the jamming attack and adapting the data transmission mode (modulation and coding levels) to the successful transmission probability. To detect jamming attack correctly, it measures PDR (Packet Delivery Ratio) with SS (Signal Strength). When a node detects jamming attack, it uses our proposed new robust rate adaptation scheme for the data transmission.

The rest of this paper is organized as follows. We introduce various jamming attack strategies in Section 2. In Section 3, we describe concepts, mechanisms introduced in our jamming attack detection scheme, and rate adaption scheme. Simulation environments and performance evaluations are described in Section 4. Finally, Section 5 concludes the paper.

2. Proposed Scheme

2.1. Detection of Jamming Attack

Tactical area jamming attack can have significant effects on combat outcome. The jammer wants to disrupt communications without being detected. Therefore, the continuous jammer and the deceptive jammer are not suitable. Thus, random jamming with signal monitoring will be used in this study as it is more difficult to detect than periodic jamming. In our simulation model, the jammer injects radio signal for a random duration with a random time interval. There are many different jamming attack strategies that naturally lend themselves to detect jamming, such as signal strength, carrier sensing time, and packet delivery ratio. To detect jamming attack, we choose PDR (Packet Delivery Ratio) and SS (Signal Strength) as the jamming attack metrics for our system [7]. In a normal scenario with no interference, high SS corresponds to a high PDR. However, if the SS is low, the PDR will also be low. On the other hand, a low PDR does not necessarily imply low SS: it may be that all of a neighbor nodes have died (perhaps from consuming battery resources or devices faults), or the node is jammed. The key observation here is that in the jammed case, the SS should be high and the PDR is low.

Using these observations, we utilize a multimodal consistency check for jamming detection. Each node compares the value (PDR, SS) with the SS threshold and PDR threshold. The thresholds are decided by experiments [7]. Our jamming attack detection scheme decides that the channel is jammed if the measured SS value is higher than signal strength threshold and PDR values are lower than PDR threshold.

2.2. Rate Adaptation Scheme

Most of widely used jamming attack solutions have some limitations. Those solutions use spatial or spectrum diversity to cope with the jamming attack. These schemes do not utilize the jammed channels, though they have enough bandwidth for the data transmission. We propose a new rate adaptation scheme to overcome problems in previous works.

The most important goal of the proposed scheme is to achieve high link utilization by adjusting the transmission mode based on the expected maximum throughput, *G*. The expected maximum throughput must consider the successful transmission probability, p_s^m. Suppose that L_{Data} is the length of data frame and T_{Data}^m is the transmission time of data frame in a specific transmission mode, m. Each transmission mode specifies the transmission rate appropriately adapted to network condition. Equation (1) shows that the expected maximum throughput, G^m.

$$G^m = \frac{L_{Data}}{T_{Data}^m} \times p_s^m \tag{1}$$

The successful transmission probability can be calculated using error probabilities for a data frame and ACK frame. Suppose that $p_e^m(L_{Data})$ and $p_e^m(L_{ACK})$ are the error probabilities for a data frame and ACK frame. Equation (2) shows the successful transmission probability, p_s^m .

$$p_s^m = (1 - p_e^m(L_{Data}))(1 - p_e^m(L_{ACK})) \tag{2}$$

An ACK frame which is usually much shorter than the data frame is transmitted at the rate equal to or lowers than the data frame rate. Therefore, the error probability of the ACK frame is much lower than that of the data frame. Hence we can approximate the successful transmission probability, p_s^m into Equation (3),

$$p_s^m \approx (1 - p_e^m(L_{Data})) \tag{3}$$

The error probability for a data frame can be calculated using error probability of the PLCP (Physical Layer Convergence Procedure), $p_e^m(L_{PLCP})$, and error probability of the MPDU (MAC Protocol Data Unit), $p_e^m(L_{MPDU})$. Equation (4) shows the error probability for a data frame, $p_e^m(L_{Data})$.

$$p_e^m(L_{Data}) = 1 - [(1 - p_e^m(L_{PLCP}))(1 - p_e^m(L_{MPDU}))] \tag{4}$$

Our proposed scheme selects the transmission mode based on the expected maximum throughput, G^m. Each node is able to calculate the expected maximum throughput for each transmission mode m from a set of available transmission modes, M. Finally we can choose the optimal transmission mode, $m*$ [8]. Equation (5) shows the optimal transmission mode, $m*$

$$m^* = \arg\max_{m \in M}(G^m) \tag{5}$$

3. Performance Evaluation

In this section, the evaluation of the proposed scheme in terms of end-to-end delay and throughput is described. Simulations have been conducted using OPNET Modeler 16.0 [9]. We compare the proposed scheme with jammed area mapping scheme [10]. In order to implement proposed robust rate adaptation scheme, we modify IEEE 802.11 DCF (Distributed Coordination Function) scheme in OPNET Modeler. The simulation parameters are summarized in Table 1.

Table 1. Simulation Parameters

Parameters	value
Simulation area	5 Km × 5 Km
Transmission rage	2 Km
Traffic model	CBR
Transmission data rate	1 Mbps
Simulation time	1000 second
Signal strength threshold	-73 dBm
PDR threshold	65 %

In a network topology, 20 nodes are randomly distributed in a 5 Km × 5 Km field, and one source node broadcasts packets to 10 multicast receivers. Nodes move around based on random waypoint mobility model in which the maximum and the minimum node speeds are 50 m/s and 10 m/s, respectively, with 1 second of pause time. Figure 1 shows an example of topology.

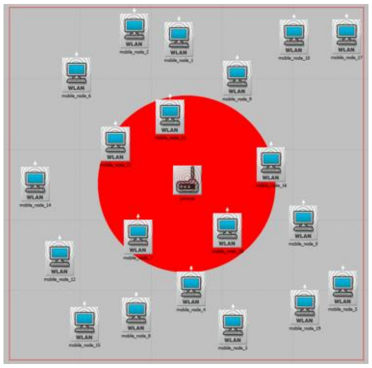

Figure 1. Network Topology

The area of a circle is the jamming area where the jammer applies to random jamming scheme at random time and with random intervals. Figure 2 shows the PDR comparison between the jammed area mapping scheme and our proposed scheme with random jamming attack. In the PDR simulation result, the proposed scheme delivers 85% packets even under serious jamming. The jammed area mapping scheme maintains over 90% PDR under less than 50% of jamming loss, but the performance rapidly degrades under more than 50% of jamming loss. Finally, the PDR drop to 70% with 90% of jamming loss while the proposed scheme keeps 85% packet delivery. Our proposed scheme quickly detects jamming attack and also selects the optimal transmission mode so that it has a better performance in terms of PDR.

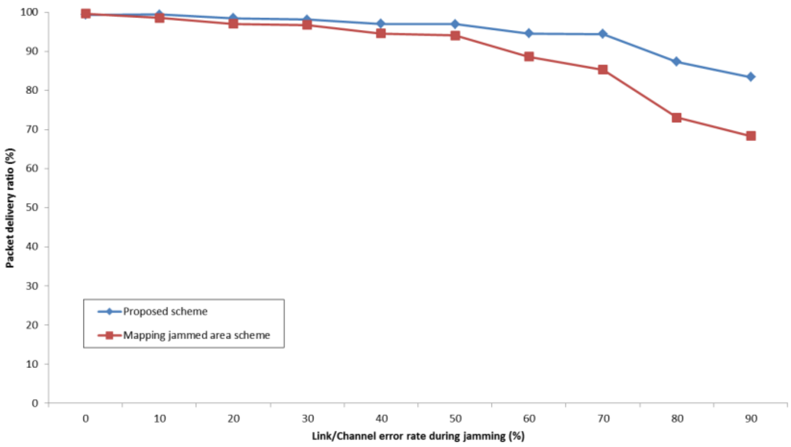

Figure 2. Comparison on PDR of each Scheme

Figure 3 shows the comparisons on the average end-to-end delay between the jammed area mapping scheme and our proposed scheme with random jamming attack. Like the PDR simulation result, our proposed scheme outperforms the jammed area mapping scheme. The Jammed area mapping scheme measures the signal strength for the detection of jamming attack. When a node detects jamming attack, it sends packets on different path by detour the jamming area, so that the jammed area mapping scheme has a high average end-to-end delay by increasing the number of hops for the data transmission.

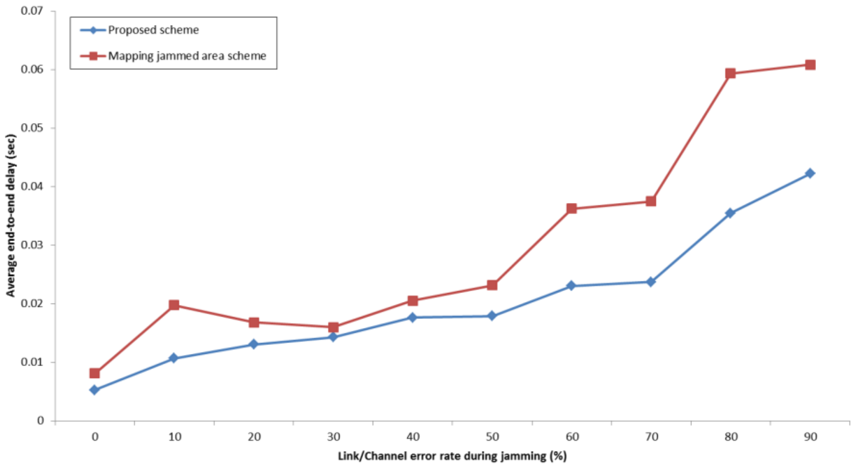

Figure 3. Comparison on end-to-end Delay of each Scheme

5. Conclusion

In this paper, we propose a new robust rate adaptation scheme that is resilient to jamming attack in a wireless multi-hop tactical network. It improves the wireless link utilization by detecting the jamming attack and adapting the data transmission mode to the successful transmission probability. In order to achieve improved the wireless link utilization in jamming attack area, our proposed scheme is selects the optimal transmission rate mode.

In order to evaluate the performance of the proposed rate adaptation scheme, we compare the rate adaptation scheme with jammed area mapping scheme. The results shown the proposed scheme quickly detects jamming attack and also selects the optimal transmission mode so that it has a better performance in terms of average PDR and average end-to-end delay.

Acknowledgements

This work was supported by Agency for Defense Development under the contact UD100023ID.

References

[1] S. Y. Oh, E. K. Lee and M. Gerla (Eds.), “Adaptive Forwarding Rate Control for Network Coding in the Tactical MANET”, Proceedings of Military Communications Conference, **(2010)** October 31-November 3; California, USA.

[2] S. Jiang and Y. Xue (Eds.), “Optimal Wireless Network Restoration under Jamming Attack”, Proceedings of 18th International Conference on Computer Communications and Networks, **(2009)** August 3-9; Francisco, California.

[3] X. Liu (Eds.), “SPREAD: Foiling Smart Jammers Using Multi-Layer Agility”, Proceedings of 26th IEEE International Conference on Computer Communications, **(2007)** May 6-12; Boston, USA.

[4] V. Navda, A. Bohra, S. Ganguly and D. Rubenstein (Eds.), "Using Channel Hopping to Increase 802.11 Resilience to Jamming Attacks", Proceedings of 26th IEEE International Conference on Computer Communications, **(2007)** May 6-12; Boston, USA.

[5] G. Noubir and G. Lin (Eds.), "Low-Power DoS Attacks in Data Wireless LANs and Countermeasures", Proceedings of ACM SIGMOBILE Mobile Computing and Communications Review, **(2003)**, Vol. 7, Issue. 3.

[6] W. Xu, K. Ma, W. Trappe and T. Zhang (Eds.), "Jamming Sensor Networks: Attack and Defense Strategies", Proceedings of IEEE Network, **(2006)**, Vol. 20, Issue. 3.

[7] W. Xu, W. Trappe, Y. Zhang and T. Wood (Eds.), "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", Proceedings of 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, **(2005)** May 25-27; Illinois, USA.

[8] K. Ju and K. Chung (Eds.), "Robust Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks", Proceedings of 6th International Conference on Information Security and Assurance, **(2012)** April 28-30; Sanghai, Chaina.

[9] OPNET, http://www.opnet.com.

[10] A. D. Wood, J. A. Stankovic and S. H. Son (Eds.), "JAM: A Jammed-Area Mapping Service for Sensor Networks", Proceedings of 24th IEEE Real-Time Systems Symposium, **(2003)** December 3-5; Cancun, Mexico.

Authors

Kwangsung Ju received the B.S. degree from Kwangwoon University, Seoul, Korea, from Communications Engineering Department in 2010. Currently he is pursuing Ph.D. degree in Communications Engineering Department at Kwangwoon University. His research interests include MANET, QoS mechanism, and video streaming.

Kwangsue Chung received the B.S. degree from Hanyang University, Seoul, Korea, M.S. degree from KAIST (Korea Advanced Institute of Science and Technology), Seoul, Korea, Ph.D. degree from University of Florida, Gainesville, Florida, USA, all from Electrical Engineering Department. Before joining the Kwangwoon University in 1993, he spent 10 years with ETRI (Electronics and Telecommunications Research Institute) as a research staff. He was also an adjunct professor of KAIST from 1991 to 1992 and a visiting scholar at the University of California, Irvine from 2003 to 2004. His research interests include communication protocols and networks, QoS mechanism, and video streaming.