Robust Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks

Kwangsung Ju, Kwangsue Chung

Department of Communications Engineering
Kwangwoon University
Seoul, Korea
Email: 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.

Keywords: Wireless tactical network, Jamming attack, Rate adaptation.

1 Introduction

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 [2-4]. If nodes find the jamming attack, they send packets on a detour [2] or switch communication channel [4]. 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.

2. Proposed Scheme

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 [5].

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. 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.

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 proba-

bility of the MPDU (MAC Protocol Data Unit), $p_e^m(L_{MPDU})$. Equation (4) shows the error probability for a data frame, $p_e^m(L_{Data})$.

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

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^*. Equation (5) shows the optimal transmission mode, m*

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

3 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.

Our future work includes the performance evaluation of the proposed robust rate adaptation scheme in various jamming attack scenario.

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

References

1. Oh, S.Y., Lee, E.K., Gerla, M.: Adaptive Forwarding Rate Control for Network Coding in the Tactical MANET. In: Military Communications Conference, pp. 1381--13864. (2010)
2. Jiang, S,. Xue, Y.: Optimal Wireless Network Restoration under Jamming Attack. In: 18th International Conference on Computer Communications and Networks, pp. 1--6. (2009)
3. Liu, X,. Noubir, G., Sundaram, R., Tan, S.: Spread: Foiling Smart Jammers using Multi-Layer Agility. In: 26th IEEE International Conference on Computer Communications, pp. 2536--2540. (2007)
4. Navda, V,. Bohra, S., Ganguly, S., Rubenstein, D.: Using Channel Hopping to Increase 802.11 Resilience to Jamming Attacks. In: 26th IEEE International Conference on Computer Communications, pp. 2526--2530. (2007)
5. Xu, W,. Trappe, W., Zhang, Y., Wood, T.: The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. In: 6th ACM international symposium on Mobile Ad hoc Networking and Computing, pp. 46--57. (2005)