Abstract—In this paper, we propose a novel multicast network coding protocol that is resilience to jamming attack in a tactical wireless ad hoc network. Wireless communication is prevailed in the tactical field between military agents and vehicles, but it is fragile by jamming attack from an adversary due to the wireless shared medium. A Jammer can easily disturb other wireless communications within radio range continuously emitting radio signal. 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. We exploit packet redundancy in network coding coping with jamming. Our scheme dynamically changes the level of redundancy adapting to channel condition locally. Say, in normal situation, it decreases a forwarding rate to save resources, but an intermediate node injects more encoded packets while jamming attack occurs. We provide performance evaluations of resiliency and efficiency of the new scheme via simulation study.

I. INTRODUCTION

Since the tactical MANET uses shared wireless medium, it is particularly vulnerable to jamming attacks. For example, it is known that serious disruption can be occurred to all Wi-Fi traffic within 100 meter range using a standard PDA with 802.11 [1]. Jamming is considered as a Denial of Service (DoS) attack; the adversary blocks communications by continuously injecting junk messages or signal into the shared wireless medium (thus, disrupting normal MAC layer operations or introducing packet collisions). As a result, jamming may cause widespread disruption and delays. Previous works used spatial or spectrum diversity to cope with jamming [2], [3], [4], [5], [6]: if nodes find jamming, they either switch communication channel or take a detour route. However, channel switching or detouring jamming area requires a special waveform or knowledge of the network topology. We can also overcome the attack using temporal diversity that is based on an erasure resistant source coding scheme such as Reed-Solomon and LPDC (Low Density Parity Check) codes. However, if jamming only affects a portion of the tactical field for a random period of time, source coding is not efficient because redundant packets transmissions cause congestion and bandwidth waste. Unlike source coding, network coding can dynamically generate redundant packets, allowing us to provide a different level of redundancy based on location and time.

In this paper, we propose a multicast scheme in tactical MANETs that is jamming resilient using network coding. Each node dynamically adjusts coding and forwarding rates locally based on channel condition. If channel condition becomes worse, a node generates and forwards more coded packets. To this end, each intermediate node includes its rank of the current generation in the packet header, and an up-stream node adjusts forwarding rate based on the overhead rank information of down-stream nodes. The main contributions of this paper are as follows. First, we develop a novel scheme coping with tactical area jamming attack using network coding. Our protocol does not require any other special radio system or knowledge of the network topology. Second, this is the first multicast protocol that is jamming resilience in tactical MANET scenarios. Last, we implement and run simulations to provide extensive performance evaluations of resiliency and efficiency of the protocol. We validated the effectiveness of our proposed protocol via extensive QualNet simulations.

The remainder of this paper is organized as follows: Section II describes details of adaptive forwarding scheme; Section III presents simulation results; and we conclude the paper in section IV.

II. ADAPTIVE FORWARDING

We assume that the jammer cannot fill the channel with signal completely so that more packets may penetrate if a sender increases the number of transmitted packets. Thus, we apply temporal diversity, e.g., generating redundant packets, against the jamming attack. Packet redundancy is already provided in MAC and Transport layer, ARQ and FEC, but 802.11 multicast mode does not use those techniques. Instead of ARQ and FEC, we can use other packet redundancy techniques in 802.11 multicast mode, namely erasure/rateless coding (at the end-to-end level) and network coding (at the packet forwarding level). End-to-end coding supports robustness and reliability in disruptive network condition, but it may waste resources, e.g., bandwidth, if jamming attack covers a portion of network area. Thus, we consider packet redundancy in network coding as ammunition of the tactical area jamming attack.

Unlike the source coding, all nodes in the network participate in encoding process in the network coding. A source node
splits data stream from an application into blocks, size k, and transmits packets after encoding each block via random linear coding. Intermediate nodes as well as the source can generate unlimited number of encoded packets mixing received or overheard packets and thus each node is able to have own encoding rate adapting to local channel condition. In the adaptive forwarding scheme, a node detects channel condition via a passive ack from a down-stream node. For the passive ack, nodes have a timer function that starts receiving the first packet in the generation. As soon as receiving enough packets in the generation or reaching timeout, nodes transmit re-encoded packets. Nodes except a source record rank r of the generation as well as encoding vector in the packet header and forward them. The rank indicates the number of received innovative packets in the generation. Upon overhearing a packet from the down-stream node, a node adjusts own forwarding rate and help, if \( r < k \) in the packet header, the downstream node forward more encoded packets. Forwarding rate, \( c \), is the number of packet transmission over the generation size, \( c = \frac{r}{k} \). If the down-stream node fails to complete the generation, a node linearly increases \( c \); otherwise, \( c \) decreases linearly. Forwarding rate \( c \) can be presented as following.

\[
    c_{\text{new}} = \begin{cases} 
        c_{\text{old}} + \alpha k & \text{if } r < k, \\
        c_{\text{old}} - \alpha k & \text{otherwise}
    \end{cases}
\]

where \( \alpha \) is a constant value, e.g., \( \alpha = \frac{1}{2} \) in our simulation. Adaptive forwarding has the maximum and minimum forwarding rate to prevent unlimited increasing or decreasing, e.g., \( c_{\text{max}} = 2k \) and \( c_{\text{min}} = \frac{k}{2} \) in simulations.

### III. Simulation Results

In this section, we validate adaptive forwarding using QualNet, a packet level network simulator. We implement random jamming scenario in which the jammer starts jamming random time with random period in a portion of the network area. During jamming period, nodes in the jamming area lose \( 50 \sim 90\% \) of packets. Figure 1 presents the number of transmitted packet changes under random jamming and figure 2 shows packet delivery ratio in terms of jamming level. Adaptive forwarding increases forwarding rate when jamming starts and thus shows higher delivery ratio compare to normal network coding under jamming.

### IV. Conclusion

Jamming attack in the tactical area can cause widespread disruption and have significant effects on military mission accomplishment to interfere wireless communications. In this paper, we propose a multicast scheme in tactical MANETs that is jamming resilient using network coding. A node dynamically adjusts coding and forwarding rates locally based on channel condition. In normal situation, adaptive forwarding decreases a forwarding rate to save resources and increases the number of packets forwarding only when it necessary. We find performance gain through the simulation study. For future work, we will develop the algorithm to distinguish jamming attack from normal congestion. In addition, we will implement adaptive forwarding and do experiment using multiple nodes.

### ACKNOWLEDGMENT

This research was sponsored by the U.S. Army Research Laboratory and the U.K. Ministry of Defence and was accomplished under Agreement Number W911NF-06-3-0001. The views and conclusions contained in this document are those of the author(s) and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory, the U.S. Government, the U.K. Ministry of Defence or the U.K. Government. The U.S. and U.K. Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

### REFERENCES