ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY
TECHNOLOGY

Anti-Jamming For Wireless Sensor Networks

Naveen Kumar[*1], Pankaj Kumar[2], Naveen Budshera[3], Monu Kumar[4]
[*1,2,3,4] B.Tech (Student), Department of ECE Dronacharya College of Engineering,Gurgaon-122506,India
nkyadav019@gmail.com

Abstract

Resilience to electromagnetic jamming and its avoidance are difficult problems. It is often both hard to distinguish malicious jamming from congestion in the broadcast regime and a challenge to conceal the activity patterns of the legitimate communication protocol from the jammer. In the context of energy-constrained wireless sensor networks, nodes are scheduled to maximize the common sleep duration and coordinate communication to extend their battery life. This results in well-defined communication patterns with possibly predictable intervals of activity that are easily detected and jammed by a statistical jammer. We present an anti-jamming protocol for sensor networks which eliminates spatio-temporal patterns of communication while maintaining coordinated and contention-free communication across the network. Our protocol, WisperNet, is time-synchronized and uses coordinated temporal randomization for slot schedules and slot durations at the link layer and adapts routes to avoid jammers in the network layer. Through analysis, simulation and experimentation we demonstrate that WisperNet reduces the efficiency of any statistical jammer to that of a random jammer, which has the lowest censorship-to-link utilization ratio. WisperNet has been implemented on the FireFly senor network platform.

Keywords: Jamming,WisperNet,FireFly,Routing.

Cognitive Radio Network

Jamming is the radiation of electromagnetic energy in a communication channel which reduces the effective use of the electromagnetic spectrum for legitimate communication. Jamming results in a loss of link reliability, increased energy consumption, extended packet delays and disruption of end-to-end routes. Jamming may be both malicious with the intention to block communication of an adversary or non-malicious in the form of unintended channel interference. In the context of embedded wireless networks for time-critical and safety critical operation such as in medical devices and industrial control networks, it is essential that mechanisms for resilience to jamming are native to the communication protocol. Resilience to jamming and its avoidance, collectively termed as anti-jamming, is a hard practical problem as the jammer has an unfair advantage in detecting legitimate communication activity due to the broadcast nature of the channel.

The jammer can then emit a sequence of electromagnetic pulses to raise the noise floor and disrupt communication. Communication nodes are unable to differentiate jamming signals from legitimate transmissions or changes in communicationactivity due to node movement or nodes powering off without some minimum processing at the expense oflocal and network resources.

In the case of energy-constrained wireless sensor networks, nodes are scheduled to maximize the common sleep duration and coordinate communication to extend their battery life. With greater network synchronization, the communication is more energy-efficient as nodes wake up from low-power operation just before the common communication interval. Such coordination introduces temporal patterns in communication with predictable intervals of transmission activity. Channel access patterns make it efficient for a jammer to scan and jam the channel only during activity intervals. The jammer can time its pulse transmission to coincide with the preambles of packets from legitimate nodes and thus have a high censorship to channel utilization ratio while remaining difficult to detect. The jammer is thus able to exploit the temporal patterns in communication to disrupt a transmission of longer length of legitimate transmissions with a small set of jamming pulses.

For nodes in fixed locations, a jammer can select regions with heavier communication activity or denser connectivity to increase the probability that a random jamming pulse results in corrupting an on-going transmission.

Nodes in the proximity of the jammer will endure a high cost of operation in terms of energy consumption and channel utilization with a low message delivery rate. They must either physically re-locate or increase the cost of their links so the network may adapt its routes.

Methods for anti-jamming must therefore address threats due to both temporal patterns at the link layer and spatial distribution of routes in the network layer. Our goal in designing Westerner, an anti-jamming protocol is to reduce or eliminate spatio-temporal patterns in communication while maintaining energy-efficient, coordinated and collision-free operation in multi-hop wireless sensor networks. We achieve this by incorporating coordinated temporal randomization for slot schedules and slot durations between each node and its k-hop neighbours. This prevents the jammer from predicting the epoch and length of the next activity on the channel. Such mechanisms reduce the effectiveness of any statistical jammer to that of a random pulse jammer.

While temporal randomization prevents statistical jammers from determining any useful packet inter-arrival distribution for preemptive attacks, it still has an efficiency of a random jammer and can achieve censorship which increases linearly with channel utilization and jamming activity. To avoid such random jammers which are co-located near nodes with active routes, we employ adaptive routing to select paths such that the highest possible end-to-end packet delivery ratios are achieved.

Anti-Jamming Protocol

We combine the above temporal and spatial schemes in a tightly synchronized protocol where legitimate nodes are implicitly coordinated network-wide while ensuring no spatio-temporal patterns in communication are exposed to external observers. In the context of multi-hop embedded wireless networks, which are battery-operated and require low-energy consumption, we require the following properties from the anti-jamming protocol:

Non-predictable schedules: Transmission instances(e.g. slot assignments) are randomized and nonrepeating to prevent the jammer from predicting the timing of the next slot based on observations of channel activity. In this way, even if the jammer successfully estimates slot sizes, it has to transmit pulse attacks at an interval of the average slot duration to corrupt communication between nodes.

Non-predictable slot sizes: Slots are randomlysized on a packet-by-packet basis in order to prevent the jammer from estimating the duration of channel activity for energy efficient reactive jamming. This requirement further reduces the jammer’s lifetime as it will need to employ the smallest observed slot duration as its jamming interval.

Coordinated and scheduled transmission: The communication schedule according to which a node transmits is known to all of its legitimate neighbors so they can wake up to receive the message during its transmission slot. This also prevents nodes from turning on their receiver when no legitimate activity is scheduled and hence reduces the likelihood of a jammer draining the energy of a node.

Coordinated changes of slot sizes: All nodes must be aware of the current and next slot sizes. This is very important because any incompatibility or synchronization error would disable communication between legitimate nodes.

Collision-free transmission:Communication must satisfy the hidden terminal problem so that a transmit slot of a given node does not conflict with transmit slots of nodes within its k-hop interference range.

Limitations

The WisperNet-Spatial routing scheme is centralized and will not scale well in large networks (>500 nodes) under moderate to heavy attack as the message from the gateway may not get through. While several distributed heuristics for the MST problem exist, they require a large amount of information with respect to shortest paths from a node to all other nodes in the network.

These schemes are not conducive to energy constrained and memory-constrained sensor networks. We aim toexplore distributed solutions further.

Conclusion

In this paper we proposed the WisperNet anti-jamming protocol which uses Coordinated Temporal Randomization of transmissions (WisperNet-Time) to reduce the censorship ratio of a statistical jammer to that of a random jammer.

A second component of WisperNetis Coordinated Spatial Adaptation (WisperNet-Space), where network routes are adapted continually to avoid jammed regions (and hence random jammers).

Through simulation and experiments, we demonstrate that WisperNet is able to effectively reduce the impact of statistical and random jammers. Unlike coding-based schemes, WisperNet is resilient to jamming even under moderate to high link utilization with ≤2% censorship rate for the network topologies explored in this work. The schedules derived from WisperNet are nonrepeating, with randomized packet lengths while maintaining coordinated and collision-free communication.

WisperNet has been implemented on a network of FireFly sensor nodes with tightly synchronized operation and low operation overhead.

References

[1] W. Xu, W. Trappe, Y. Zhang, and T.Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In ACM MobiHoc, 2005.

[2] W. Xu, T. Wood, W. Trappe, and Y. Zhang Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service. In ACM WiSe, pages 80–89, 2004.

[3] Y. W. Law et al. Energy-efficient link-layer jamming attacks. In ACM SASN, 2005.

[4] A. J. Viterbi. Spread Spectrum Communications: Myths and Realities. In IEEE Comm. Magazine, 2002.

[5] A. D. Wood, J. A. Stankovic, and G. Zhou. DEEJAM: Defeating Energy-Efficient Jamming. IEEE SECON, 2007.

[6] Texas Instruments Inc. Chipcon CC2420 Data Sheet, 2003.

[7] A. D. Wood, J. A. Stankovic, and S. H. Son. JAM: A Jammed Area Mapping for Sensor Networks. In IEEE RTSS, 2003.

[8] J. Polastre, J. Hill, and D. Culler. Versatile Low Power Media Access for Wireless Sensor Networks. SenSys, November 2005.

[9] W. Ye, J. Heidemann, and D. Estrin. An energy-efficient MAC protocol for wireless sensor networks. IEEE INFOCOM, 2002.

[10] A. El-Hoiydi and J. Decotignie. WiseMac: An Ultra Low Power MAC Protocol. ISCC, 2004.

[11] L.F.W. van Hoesel and P.J.M. Havinga. A lightweight medium access protocol for wireless sensor networks. INSS, 2004.

[12] A. Rowe, R. Mangharam, and R. Rajkumar. RT-Link: A Time-Synchronized Link Protocol for Energy Constrained Multi-hop Wireless Networks. IEEE SECON, 2006.

[13] T. Dam and K. Langendoen. An adaptive energy-efficient mac protocol for wireless sensor networks. SenSys, November 2003.

[14] R. Mangharam, A. Rowe, and R. Rajkumar. FireFly: A Cross-layer Platform for Real-time Embedded Wireless Networks. Real-Time System Journal, 37(3):183–231, 2007.

[15] B. Schneier. Applied Cryptography. John Willey Inc., 1996.

[16] A. Perrig and et. al. SPINS: Security Protocols for Sensor Networks. Wireless Networks, 8(5):521–534, 2002.

[17] A. Perrig, R. Canetti, D. Tygar, and D. Song. The TESLA Broadcast Authentication Protocol. Cryptobytes, 5(2), 2002.

[18] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, 1997.

[19] B. Y. Wu and Kun-Mao Chao. Spanning Trees and Optimization Problems. Chapman and Hall, CRC Press, 2004.

[20] A. Eswaran, A. Rowe, and R. Rajkumar. Nano-RK: Energy aware Resource centric RTOS. IEEE RTSS, 2005.