www.icoin.org

ICOIN 2010

The International Conference on Information Networking 2010 (ICOIN 2010)

Conference Program

January 27 (Wed) - 29 (Fri), 2010
Paradise Hotel, Busan, Korea

Sponsored by KIISE Information Network Society

한국정보과학회
Korean Institute of Information Scientists and Engineers

Supported by

OPENBASE SWRC

Technical Sessions

11:00-12:00

Session 3A (Miami Room)

Ad-Hoc Networks II

Chair: Jae Hwoon Lee (Dongkuk University, KR)

A Maximum-Revenue Multicast Routing Problem on Wireless Mesh Networks
Wen-Lin Yang (National University of Tainan, TW)

A Multi-channel MAC Protocol for Hostile Environment
Zaw Htike, Choong Seon Hong (Kyung Hee University, KR)

The IEEE 802.11-Integrated Multi-hop MAC Broadcast Protocols for VANETs
Younghyun Han, Hyukjoon Lee (Kwangwoon University, KR)

Session 3B (Venice Room)

Network Management

Chair: Yongtai Shin (Soongsil University, KR)

Fast and Accurate Node Failure Detection
Mozafar Bag-Mohammadi (University of Ilam, IR), Farzad Safaei (University of Wollongong, AU), Nasser Yazdani (University of Tehran, IR)

TECLAS - an Extremely Configurable Log Analyser System
Joao Trindade, Teresa Vazao (Instituto Superior Tecnico, PT)

Tooldiag: Design and Implementation of Bulk Data Transfer Tool Performance Diagnosis System in High Speed Networks
Young-Ju Han, Min-Woo Park (Sungkyunkwan University, KR), Jong-Myoung Kim (KISA, KR), Yoonjoo Kwon (KISTI, KR), Tai-Myoung Chung (Sungkyunkwan University, KR)

13:00-15:00

Session 4A (Miami Room)

Mobility Management

Chair: Gour C. KARMAKAR (Monash University, AU)

Design and Implementation of NEMO-based Path Aggregation using Mobile Routers on Multiple Vehicles
Kei Tanimoto, Susumu Ishihara (Shizuoka University, JP)

Improvement of Link Detection for the Power Conservative Multi-radio Terminal
Hyunho Park, Junghoon Jee, Changmin Park (ETRI, KR)

Localized Management for Proxy Mobile IPv6
Seok Hyun Hwang, Jin Ho Kim, Choong Seon Hong (Kyung Hee University, KR), Jung-Sik Sung (ETRI, KR)

GLSS: Grid-based Location Service Spot Scheme for Optimized Routing Path on VANET
Jonghyun Kim, MiYoung Jo, Yunho Jung, Keecheon Kim (Konkuk University, KR)

Context Profile Handling Mechanism for Source Specific Multicast in Proxy Mobile IP
JooHyung Lee, S.H. Shah Newaz, JongMin Lee, JunKyun Choi (KAIST, KR)

Session 4B (Venice Room)

Quality-of-Service

Chair: Frank Bohdanowicz (University of Koblenz, DE)

A Fuzzy Dropper to Provide Proportional Loss Rate Differentiation in a Wireless Network with a Multi-state Channel
Yu-Chin Szu (St. John's University, TW)

A Codec-based QoS Support for IP Networks
Seong-Ho Jeong (Hankuk University of Foreign Studies, KR), Ki-Jong Koo, Tae-Gyu Kang, Hyun-Joo Bae (ETRI, KR)

On Improving the Fairness of Active Queue Management for Congestion Control
Jahon Koo, Kwangsue Chung (Kwangwoon University, KR)

A Bottleneck and Target Bandwidth Estimates-Based Congestion Control Algorithm for High BDP Networks
Tuan-Anh Le, Choong Seon Hong (Kyung Hee University, KR)

QoS Method based on Utility Function for Cellular Network
Shintaro Uno (Kanazawa Institute of Technology, JP), Kwang Sik Kim, Moo Wan Kim (Tokyo University of Information Sciences, JP), Shunji Abe (National Institute of Informatics, JP)

15:30-17:30

Session 5A (Miami Room)

Sensor Networks

Chair: Seong-Ho Jeong (Hankuk University of FS, KR)

A Grid-based Rerouting Method for Mobile Sinks in WSNs
Jieun Cho, Jongwon Choe (Sookmyung Women's University, KR)

Area Coverage Patterns for Node Scheduling Problem to Extend the Network Lifetime
Ngoc Duy Nguyen, Vyacheslav Zalyubovskiy, Minh Thiep Ha, Hyunseung Choo (Sungkyunkwan University, KR)

On Interactions between Routing and Service Discovery in Wireless Sensor Networks
Ari Karjalainen (University of Helsinki, FI), Jussi Kangasharju (Helsinki Institute for Information Technology, FI)

Data Correlation Aware Cooperative MISO Technique in Wireless Sensor Network
Mohammad Rakibul Islam, Jinsang Kim (Kyung Hee University, KR)

Impact of Duty Cycle Energy Efficiency and Performance in Wireless Sensor Networks
Bipula Khatiwada, Sangman Moh, Ilyong Chung (Chosun University, KR)

Session 5B (Venice Room)

Wide Area Networks

Chair: Yunju Baek (Pusan University, KR)

A Routing Scheme and a New Addressing Scheme for Future Network

A Multi-channel MAC Protocol for Hostile Environment

Zaw Htike, Choong Seon Hong

Department of Computer Engineering, Kyung Hee University,
1 Seocheon,Giheung, Yongin, Gyeonggi, 449-701 Korea
htike@networking.khu.ac.kr
cshong@khu.ac.kr

Abstract

Denial-of-Service (DOS) attacks are serious threats in wireless networks. The most effective and easiest DOS attack is radio jamming which simply blocks the channels with radio signals and forge packets. It is difficult to mitigate this kind of attacks since the attacker's ultimate aim is to degrade the performance of the network, not to utilize it. But we can mitigate it by simply avoiding the attack. In this paper, we propose a multi-channel MAC protocol to mitigate the jamming attacks. It is reactive autonomous channel switching mechanism. Therefore, channel switching occurs only when jamming is detected on the currently used channel. Our protocol also follows the 802.11 principle and it can be used in hostile environment.

1. INTRODUCTION

In wireless network, radio jamming attacks are difficult to prevent and protect against. Attackers need no or basic knowledge of MAC and PHY layers to launch radio jamming attacks. The adversaries can simply transmit radio signals or forge packets to disturb the transmissions of legitimate users which lead to denial of service (DOS). We can detect this kind of jamming attacks [1] [2] [3] but it is impossible to penalize the attackers who intend in DOS only. The best way to mitigate radio jamming is simply avoiding the attacks.

In this paper, we propose a multi-channel MAC protocol that can mitigate the jamming attacks and it based on the 802.11 DCF. The proposed protocol will follow the existing classic 802.11 principles if there is no jammer in their transmission ranges. When the jamming attack is detected, a node, sender or receiver, will select an un-jammed channel and migrate to it. The other node will switch and find that selected channel. The channel switching mechanisms for each node are independent. But according to our proposed mechanism, two nodes will rendezvous at an un-jammed channel after performing the channel switching mechanism.

2 .1 Motivation

Many multi-channel schemes for thwarting the jamming attacks have been proposed [4] [5] [6] [7]. But most of the multi-channel MAC protocols use a control (common) channel that can be used for channel selection and negotiation [5]. So, the attackers can simply target the control (common) channel and no potential data communication will be successful in other channels.

Moreover, the channel hopping sequence used by legitimate communication is pre-defined by a pseudo-random sequence with assumption that all legitimate nodes are reliable and the sequence is not known to the jammers [6] [8] [7]. So, it is efficient till the pseudo-random sequence remains secret. If one or two of legitimate nodes compromise with the attackers, the sequence will be useless and the attackers can attack the network with the lowest power consumptions. In our proposed protocol, we tried to overcome these two vulnerabilities. There is no control channel and no channel is predefined for the potential transmissions. When jamming attack is detected, the legitimate devices simply migrate to an un-jammed channel and continue the transmission till next jamming attack is detected on that channel.

On the other hand, IEEE 802.11 standard already has multiple channels available for use. IEEE 802.11b physical layer (PHY) has 14 channels, 5MHz apart in frequency .But to be totally non-overlapping and thus feasible for use in the same region, the frequency spacing must be at least 30MHz. So channels 1, 6 and 11 are typically used for communication in current implementations, and thus we have 3 channels available for use. IEEE 802.11a provides 12 channels, 8 in the low part of the band for indoor use and 4 in the upper part for outdoor use [12].

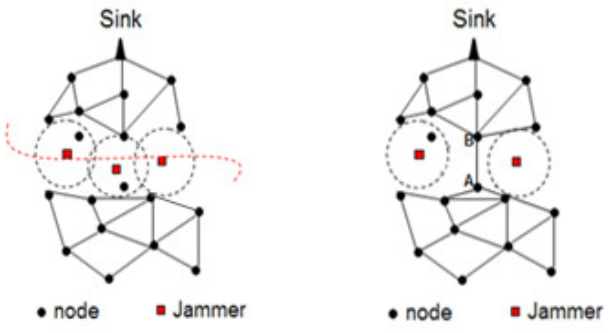
2.2 Related Work

In [7], channel hopping technique was studies in 802.11 networks. Jamming detection for sensor networks was studied in [9], and they use channel's utility to detect jamming, and their studies was focus on the issue of mapping the jamming area. The authors of [1] introduced four kinds of jammers: constant jammer, deceptive jammer, random jammer and reactive jammer, and their impacts. They also proposed two solutions, channel surfing and spatial retreats [6]. Channel surfing involves valid participants changing the channel they are communicating on when a denial of service is occur. Spatial retreats involve legitimates network devices moving away from the adversary. In [2], they explored two different approaches to channel surfing: coordinated channel switching, in which the entire sensor network adjusts its channel; and spectral multiplexing, in which nodes in a jammed regions

This research was supported by the MKE, Korea, under the ITRC support program supervised by the NIPA)" (NIPA-2009-(C1090-0902-0016)) Dr. Cs Hong is corresponding author.

switch channels and nodes on the boundary of a jamming region act as radio relays between different spectral zones. The problems of jamming detection were also studied in [10] [11].

The authors of [5] addressed the problem of control channel jamming attack in multi-channel networks. They used more than one control channels to mitigate the attacks. They also described the impacts of the jamming attacks. It showed that the network can be partitioned by the jammers and sometime it is forced to route through specific path as shown in Figure 1. It is very difficult to reconstruct the network when it is partitioned if single channel is used. Furthermore no communication will be successful in jamming area as long as the jammers are present. The spatial retreat might not be used efficiently in this saturation.



(a) (b)

Fig. 1: (a) the jammers partitions the network into two parts (b) the adversary forces all traffics to pass through the link *(A, B)*

3. The Proposed Multi-channel Protocol

In our scheme, two communication host, transmitter and receiver, periodically exchange the preambles to make sure the present channel can be used for data transmission. When the sender wants to send data packets, it will simply follow the classic 802.11 principle as shown in Figure 2.

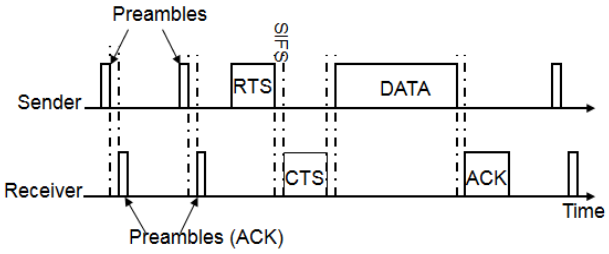
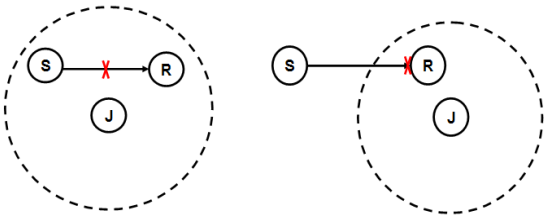


Fig. 2: Normal operation before the jamming attack is detected

The sender sends RTS and the receiver replies CTS. And the sender sends Data packet and the communication will be successfully terminated by sending back the ACK. If there is no data to send, the nodes exchange the preambles periodically. This operation will be performed repeatedly till the jamming attack occurs. When the jamming attack is detected, both sender and receiver will move to un-jammed channel and continue the operation.

3.1. Problem Statement

The attacker might be in the transmission ranges of both sender and receiver or it may target only one node, receiver or sender. Figure 3 (a) shows that the attacker, J, transmits radio signals in order to interference communication between S and R. In this case, both S and R are in the transmission range of jammer. So, both nodes can detect the attack and they can move to other channel simultaneously. But in Figure 3 (b), the attacker (J) targets to the receiver (R) and the sender (S) cannot detect the jamming of J. When R detects the interference from J, it will simply avoid the attack and move to un-jammed channel. But S does not know that R is on the other channel because it cannot detect the jamming from J when R detects. Synchronization will be problem in this case. In our protocol, we do not force the sender and receiver to switch the channel at the same time. The nodes can switch the channel independently.



(a) (b)

Fig. 3: (a) jammer (J) transmits the radio signal in order to interfere the communication between sender (S) and receiver (R), (b) attacker only targets to receiver (R)

3.2. Channel Switching Mechanism

We classify the nodes into two groups: channel selector and sweeper. The main duty of channel selector is to select the channel and wait the sweeper after migrating to the new channel. The sweeper has to switch and find the channel which the selector is present.

When jamming attack is detected, the selector will select an un-jammed channel from its channel list and migrate to it (channel selection and jamming detecting mechanisms will be presented in 3.3). The selector will stay on the selected channel and wait for the sweeper with definite time interval T_W. T_W is the total time for the selector to stay on one channel and it can be calculated as:

$$T_W = (N-1)\, T_S + (N-2)\, \beta \quad (1)$$

In this case, N denotes total number of channels and β is channel switching time. T_S refer the maximum time that the sweeper spends on one channel. T_S can be defined as:

$$T_S = 2\,(T_P + SIFS + \partial) \quad (2)$$

T_P denotes the preamble transmission time and ∂ is the propagation delay.

The sweeper will also migrate to one of the un-jammed channel after jamming attack is detected. And it will switch one channel after another except the previous channel which is being jammed and find the channel which is selected by the selector. After migrating to an un-jammed channel, the sweeper broadcasts the preamble after SIFS and waits for the preamble (ACK) from the selector. After broadcasting preamble, the sweeper waits specific time interval which is equal to T_O ($T_O = T_S - (T_P + SIFS)$) and if it does not receive the preamble (ACK) within the specific time, it will determine that the selector is not present on this channel. So, the sweeper will switch to another un-jammed channel, broadcast the preamble again and wait preamble (ACK) and so on. This operation will be routine till the selector is found on one channel. Figure 4 is shown as an example of channel switching mechanism.

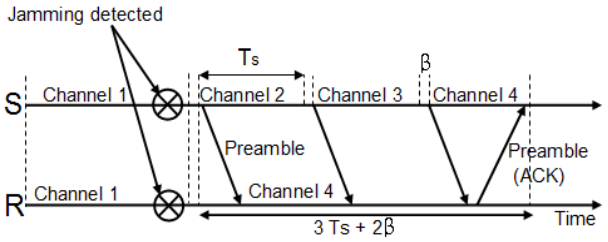


Fig. 4: S switches and finds the channel which R is present

In Figure 4, the receiver (R) is the selector and sender (S) stands for the sweeper. Before any jamming attack is detected, the communication nodes use the channel 1 and operate as shown in Figure (2). After detecting the jamming attack, the receiver (selector) moves to the channel 4 and waits T_W time for the sender (sweeper).

The sender (sweeper) shall also switches to an un-jammed channel, channel 2, after detecting jamming attack at present channel. The sender checks if selector is present in this channel by sending preamble. In this case, if the sender does not receive preamble (ACK) at channel 2 within timeout T_O and it will move to channel 3 to find the receiver and so on. When the sender reaches to channel 4, it transmits preamble as usual. The receiver replies preamble (ACK) after getting preamble from sender and the sender determines that this channel is the one which the receiver is present. Finally the sender and receiver rendezvous at channel 4. Both nodes are going to use the channel 4 for potential communication till the next jamming attack is detected.

Two nodes might not switch channel at the same time. When only one node, sender or receiver, is being jammed, the jamming attack might not be detected by both nodes simultaneously as shown in Figure 3 (b). And the available channels for each node might not be the same. For example, a channel which is selected by receiver (selector) might not be available for the sender (sweeper) because it might currently be jammed by another jammer. So, the selector will also migrate next channel if it dose not receive any preamble after waiting a definite time interval (T_W) at one channel.

In Figure 5, the receiver switches to channel 4 after the jamming attack is detected. But the sender leaves the jammed channel one or two time slots lately and the channel 4 might not be available for sender, so it switches only channel 2 and 3 and the receiver will receive no preamble in its first time slot. So, after waiting a T_W, the receiver moves to another un-jammed channel, channel 3, and waits again. The sender will be routine its function till the receiver is found. So, the sender and receiver will rendezvous at channel 3 if it is available for both nodes although they switched the channels independently.

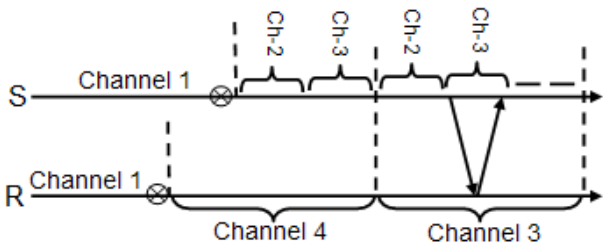


Fig. 5: The sender and receiver rendezvous at channel 3 although the channel selecting and switching time are different.

3.3. Jamming Detection and Channel Selection

We assume that the environment is hostile and the attacker might appear anytime. So, the legitimate nodes periodically exchange the preambles and each node senses the carrier on all channels and maintains the channel list according to the power it senses. The channel with lowest power level will be top of the list and the nodes will switch one channel after another according to their own channel list. Thought this does not guarantee that all channel lists can be the same. But it is likely to be the same at that location and it serves high probability to meet two nodes at the same channel within short period.

When the preamble absence occurs, node will monitor the time spent sensing the channel [3], and if it senses high power level within that time, it will determine that the channel is being jammed and moves to un-jammed channel immediately, because high power level should correspond to high throughput. Otherwise it will stay on the same channel and

waits for next preamble. But it does not guarantee that the jamming signal will last long enough to be sensed by the nodes. Therefore we also suggest defining the PDR threshold which can be determined by calculating the number of preambles received at each node. As soon as the PDR of preamble is below the threshold, the node will leave the present channel although it did not sense high power level.

The attacker might be reactive and only targets to data communications. It overhears the RTC/CTS packets and estimates when the data packet will be transmitted. So, it transmits radio signals while the data packet is being sent. It results the collision and the data packet will be lost. So, after transmitting CTS, the receiver computes a timeout, while it is expecting a data packet from the transmitter [12]. If the data does not arrive within this timeout, it will assume the channel is not reliable or being jammed although the data packet might be lost accidentally or intentionally. At the sender side, after transmitting the data frame, it computes a timeout for ACK, if no ACK is received from the receiver within that definite time interval, it will also determine that the channel is not reliable. In this case, both sender and receiver might leave the channel simultaneously.

4. Discussion

The main goal of our protocol is to avoid the jamming attacks. When nodes detect the jamming attack on currently used channel, they will stop any communication on jammed channel and try to reconstruct the network on other un-jammed channel. While the network is under reconstruction, which means that the channel switching mechanism is being performed, the throughput of the network might be zero. The time needed for reconstruction the network depends on total channels available of nodes. The more channels it uses the longer the network reconstruction time. But, it will make more difficult for the attacker to attack the network effectively. Thus, the performance of the protocol depends on the number of total channels that nodes use and the number of jammers present in its environment. Nonetheless, according to our proposed mechanism, if there is even only one available channel for both nodes, the operation can be performed well as a normal environment.

5. Conclusion and Future Work

In wireless network, jamming is pretty easy since the devices use single channel communication. We just proposed a multi-channel concept to mitigate the jamming attacks and intended to use in hostile environment. We also tried to overcome two vulnerabilities, using control channel and pseudo-random sequence, which are commonly used in most of multi-channel protocol. We also aimed to use our protocol to operate on existing classic 802.11 LAN environments. As a future work, we will try to extend our multi-channel concepts on multi-hop and ad hoc networks.

REFERENCES

[1] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network,* vol. 20, pp. 41-47, 2006.

[2] W. Xu, W. Trappe, and Y. Zhang, "Defending wireless sensor networks from radio interference through channel adaptation," *ACM Transactions on Sensor Networks* 2008.

[3] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *6th ACM international symposium on Mobile ad hoc networking and computing*, 2005, pp. 46-57.

[4] G. Alnifie and R. Simon, "A multi-channel defense against jamming attacks in wireless sensor networks," in *3rd ACM workshop on QoS and security for wireless and mobile networks*, 2007, pp. 95-104.

[5] L. Lazos, S. Liu, and M. Krunz, "Mitigating control-channel jamming attacks in multi-channel ad hoc networks," in *second ACM conference on Wireless network security*, 2009, pp. 169-180.

[6] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service," in *3rd ACM workshop on Wireless security*, 2004, pp. 80-89.

[7] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in *IEEE INFOCOM 2007*, 2007, pp. 2526-2530.

[8] J. Mo, H. S. W. So, and J. Walrand, "Comparison of multichannel mac protocols," *IEEE Transactions on mobile computing,* vol. 7, pp. 50-65, 2008.

[9] A. D. Wood, J. A. Stankovic, and S. H. Son, "JAM: A jammed-area mapping service for sensor networks," in *24th IEEE Real-Time Systems Symposium*, 2003, pp. 286-297.

[10] A. Sampath, H. Dai, H. Zheng, and B. Y. Zhao, "Multi-channel jamming attacks using cognitive radios," in *Computer Communications and Networks, 2007. ICCCN 2007*, 2007, pp. 352-357.

[11] A. D. Wood, J. A. Stankovic, and G. Zhou, "DEEJAM: Defeating energy-efficient jamming in IEEE 802.15. 4-based wireless networks," in *SECON '07*, 2007, pp. 60-69.

[12] L. Guang, C. Assi, and Y. Ye, "DREAM: A system for detection and reaction against MAC layer misbehavior in ad hoc networks," *Computer Communications,* vol. 30, pp. 1841-1853, 2007.