The Flaw Attack to the RTS/CTS Handshake Mechanism in Cluster-based Battlefield Self-organizing Network

Zemao Zhao

College of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China

National key laboratory of Information Control Technology in Communication System, Jiaxing 314001, China
E-mail: zhaozm@hdu.edu.cn

Fei He & Rui Xu

College of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China

The research is supported by the Research Foundation of National Key Laboratory of Information Control Technology in Communications System (No.9140C1302010802)

Abstract

In this paper, for a battlefield self-organizing network the security flaw of RTS/CTS handshake mechanism will be analyzed based on its hierarchical and clustering features. By utilizing the fact that Cluster-type structure is easily to lead to the false blocking problem, a Denial of Service attack method is proposed. In this method, the attacker utilizes the pair nodes to forge malicious information, and thus, the communications among the nodes in the same cluster are blocked. Moreover, a defense strategy against the proposed attack is presented. The simulations with NS-2.33 show that the throughput descends largely in the attacking state, and when the defense strategy is implemented, the situation that the throughput descends could be improved obviously.

Keywords: Self-organizing network, RTS/CTS handshake mechanism, Denial of service, Flaw attack

1. Introduction

The battlefield self-organizing network is generally divided into the plane structure and the hierarchical structure. The latter has many advantages such as good extension performance, unlimited scale, orientation, and mobile management, and it is more fitter for the battlefield self-organizing network than the plane structure. In the battlefield self-organizing network with hierarchical structure, the nodes with same characteristic (such as a team or a line) could be brought into one cluster for the consistent action and control. The Near Term Digital Radio (NTDR) has used two-level hierarchical structure. The application of the self-organizing network in the military domain makes its security problems in structure and protocol face large testing.

In 2003, S Ray et al. (S Ray, J B Carruthers and D Starobinski. 2003) investigated the false blocking problem and proposed a solution of RTS validation technique, and they described and analyzed this solution more exactly in (S Ray, D Starobinski. 2007). In the same year, D Chen et al. (D Chen, J Deng and P K Varshney. 2003) researched the spurious RTS/CTS attack and NAV attack, and they introduced a misbehaving node to carry out the false blocking attack based on “false blocking problem”. In 2005, J Deng et al. (J Deng, Z Zhang, S Pagadala, et al. 2005) investigated the spurious CTS attack. In the same year, Lei Guang et al. (Lei Guang, Chadi Assi. 2005) proposed two types of attacks for 802.11DCF, and one was that the attacker periodically abandoned RTS frame or DATA package, and the other was that the private node didn’t follow the MAC protocol, selected smaller contention window (CW) to attack continually or periodically, and to obtain unfair throughout. In 2008, Chen Wei et al. (CHEN Wei, YU Lei, ZHANG Ying-zhou. 2008) investigated the attackers transmitted spurious RTS/CTS frames with sufficiently longer duration time continually in the real wireless LAN, and made legal nodes could not offer service normally. In the MAC protocol of self-organizing network, the RTS/CTS handshake mechanism is intended to solve the problems in hidden terminal or exposed terminal(G Binachi. 2000)(K Xu, M Gerla, S Bae. 2003), but the characteristic of the wireless self-organizing network different from the wireless LAN would also induce some security flaws in the RTS/CTS handshake mechanism, and relative researches have evolved this problem(B Wu, J Chen, J Wu, et al. 2007)(K Bian, J Park, and R Chen. 2006)(A Rachedi, A Benslimane. 2008)(S Djahel, F Nait-Abdesselam and F Ahsan. 2009).

Comprehensively considering many characteristics such as hierarchical and clustering structure, the range of false blocking, and the single attack is easily to be detected in the real battlefield environment, this paper proposes a Denial of Service attack that set pair attackers in the cluster, and let them conspire to transmit the spurious RTS/CTS periodically, which bring out a large-scale blocking problem. We also comprehensively utilize the Network Allocation Vector (NAV), CW and the freedom of movement for expanding the effect of attack. At last, we propose a corresponding defense solution, and validate the effective defense of this solution by the NS-2.33 simulation.

2. Structure of the battlefield self-organizing network

The hierarchical structure is usually adopted in the mobile self-organizing network of the military system. In the battlefield self-organizing network with the hierarchical structure, the network is divided into several clusters, and each cluster selects a cluster head by the certain selection algorithm to take charge of the transmission among clusters. The division and management of clusters accord with the combat units. The members in the cluster all belong to one combat unit, and they all distributed in the wireless relay range of the cluster head. The existence of the cluster makes the members in the cluster need not to maintain complex routing information, and reduce the amount of the network control information. Considering the security, anti-destroy and justice of the network, the cluster head is not fixed, and it can be selected from the members in cluster at any time. A simple 2-level hierarchical network is seen in Figure 1.

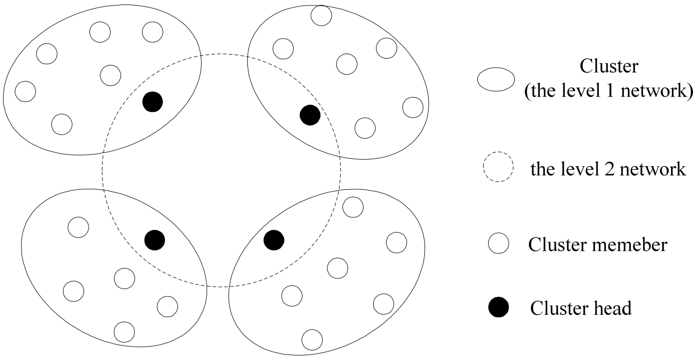

Figure 1. Clustering Structure of the 2-level hierarchical Network

The characteristics of the cluster structure include following aspects.

(1) The existence of the cluster head in the cluster structure network makes it not completely no-center.

(2) All the members in the cluster act as "group mobility" relatively to other clusters, and the members in the cluster move freely relative to the cluster head.

(3) The members in the cluster are distributed in the wireless relay range of the cluster head, and the nodes in the cluster are relatively centralized.

3. RTS/CTS flaw attack in cluster

At present, the RTS/CTS handshake mechanism and the NAV are used to solve the hidden terminal and the exposed terminal in the self-organizing network, but it also offers some methods to attack the network for attackers. Based on this cognition, the blocking attack in the cluster is proposed combining with the characteristics of the cluster structure.

3.1 Security flaws in the RTS/CTS handshake *mechanism*

First, the work process of the RTS/CTS handshake mechanism is introduced briefly as follows. In the self-organizing network based on IEEE802.11MAC, the Physical Carrier Sense(PCS) and the Virtual Carrier Sense(VCS) are adopted to decide the use of the sharing channel. Only when these two mathods show the channel is idle, the channel will be confirmed to be idle. In the VCS mechanism, each node has a NAV, it reduce the frame conflict and avoid the hidden terminal with the RTS/CTS mechanism. The RTS/CTS frame contains a duration field, which is used to set the NAV. The set of NAV in the IEEE802.11DCF is seen in Figure 2. Because when the node sets the NAV, it doesn't validate whether the value of NAV is necessary, so in fact, the node doesn't know whether the expected frame exchange occurs, which is the security flaw that the attacker could use to prevent its neighbor nodes from accessing channel.

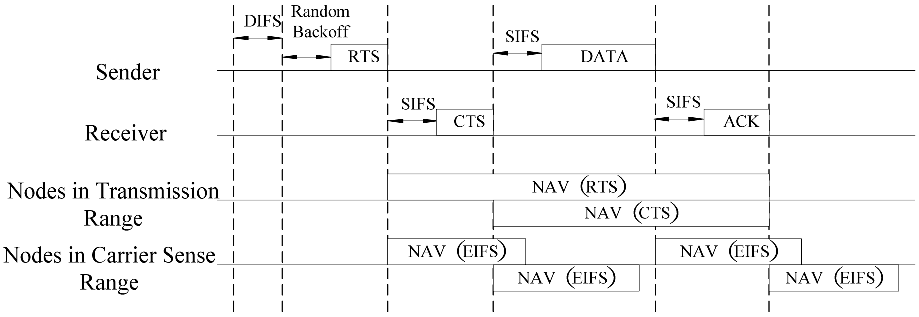

Figure 2. The Set of NAV in the IEEE802.11DCF

Because any node must defer its transmission after it overhears a RTS or CTS frame, so even the channel is idle, and the transmission of expecting data packets doesn't happen, this node will be blocked. Reference [1] described the false blocking problem induced by the failed RTS/CTS interaction without attackers in the wireless LAN, and the propagation of this problem in the network. Reference [3] proposed that the attacker would utilize the spurious RTS/CTS frame to make DoS attack in the wireless network, and introduce an misbehaving node based on the false blocking problem to randomly transmit many spurious RTS/CTS frames to a inexistent node to make its normal neighbor nodes be blocked.

3.2 Blocking attack in the cluster

We define a node to be blocked if it is prohibited from transmitting at a given instant. Channel contention and enters backoff are likely to be the reason of the node are blocked.

Suppose that the network N is composed by many nodes, and these nodes are divided into k clusters according to the environment of the battlefield. Each cluster is composed by one cluster head and many nodes. The cluster heads all belong to one level, so one two-level network forms. C_i denotes the i'th cluster, i=1, 2,…,k, and m_{ij} denotes the j'th member in the i'th cluster, j=1, 2,…s. h denotes the cluster head, and it is selected from s member nodes. The attacker A_l is acted by the captured m_{ij}. Note $N = \{C_i \mid i = 1,2,\cdots,k\}$, $C_i = \{m_{ij}, h \mid j = 1,2,\cdots,s\}$, $A_l \in m_{ij}, l < j$.

Then, according to the security flaws of the RTS/CTS handshake mechanism and the structured characteristics of the nodes in the cluster, one cluster C_i is selected randomly as the research object, and the attacker's blocking attack in the cluster can be described as follows.

(1) The selected C_i structure model is seen in Figure 3, s=15. Suppose one pair of attackers A_1 and A_2 respectively are m_{i1} and m_{i2}, their intention is to block the m_{i3} in the common transmission range of two attackers, and the blocked time is the value of NAV.

(2) A_1 and A_2 exchange the RTS/CTS. To extend the attack effect, the attacker could arbitrarily set the value of the duration in the RTS/CTS frame to reserve the channel for an addition time, and the maximum time that the channel can be reserved for a single frame is limited by the size of the duration field, i,e. 32767 µs. The attackers' intention is to falsely reset the NAV of m_{i3} , and make it to be in the blocked state for a long time. In addition, the attackers could select smaller CW to increase the opportunity to successfully occupy the channel.

(3) In the time that m_{i3} is blocked, if m_{i4} wants to communicate with m_{i3} and transmit the RTS frame, it will not get the answer frame CTS, and at the same time, all nodes in the transmission range of m_{i4} will be blocked because they would hear RTS, such as m_{i5}, m_{i6}, and m_{i15} in Figure 3. In the same way, in the time that m_{i5} and m_{i6} are blocked, if other nodes (m_{i7} and m_{i8}) transmit RTS to them, they will not get the answer frame, and their neighbor nodes will be blocked. This blocking attack could propagate throughout the whole cluster network.

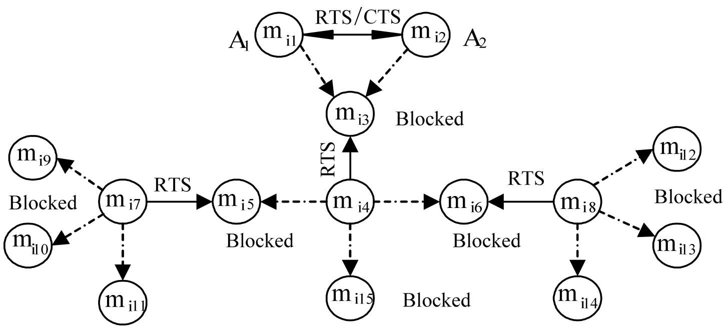

Figure 3. The Structure Model of Nodes in the Cluster

The paper induces one pair of attackers in the cluster is to make spurious RTS/CTS more easily exchange, and make attack difficult to be detected. Without attackers, the blocking problem will be automatically relieved after RTS is transmitted for certain times. But with attackers, exchanging spurious RTS/CTS frame periodically could make most nodes in the network to be in the blocked state, and the data transmission could not take place normally. Of course, to make the blocking attack act as the chain reaction, and propagate throughout the whole cluster, following conditions should be satisfied.

(1) Neighboring nodes are all in the mutual transmission range or the carrier sense range. The blocked times in the both ranges are different, because the nodes in the transmission range could decode the duration field in the RTS/CTS frame, while in the carrier sense range, the nodes couldn't, and only get the information that some signal is transmitting and the channel is busy.

(2) The time that the neighbor nodes of the blocked node transmit RTS to the blocked node must be in the blocked time. As seen as in Figure 4, m_{i4} and m_{i7} should initiate the communication at the time that m_{i3} and m_{i5} are blocked, but it has certain probability, and the concrete probability is analyzed as follows.

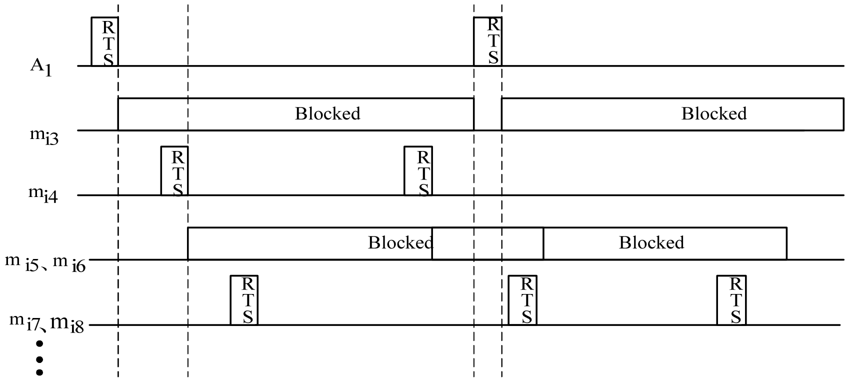

Figure 4. Time Limitation

3.3 Probability analysis

In reference [7], there are two hypotheses. (1) n terminals compete for one wireless channel, and there are not hidden terminal or exposed terminal, and various terminals always have data package to wait for transmitting. (2) In each transmission attempt, the probability p that packages collide is constant and irrelative, and the performance model of 802.11DCF is the two-dimensional discrete time Markov Chain. By analyzing the stable distribution of the two-dimensional discrete time Markov Chain, and utilize the probability normalization, the probability of a node transmits in a randomly chosen slot time is

$$\tau = \frac{2(1-2p)}{(1-2p)(W+1)+pW(1-(2p)^m)} \tag{1}$$

Where, m is the maximum backoff stage, and W is the minimum backoff window. $W=CW_{min}$, $CW_{max}=2^m W$.

Before using this conclusion to make further theoretical analysis, define

(1) T' denote the times that m_{i5} and m_{i6} are blocked, and it is decided by the RTS transmitted by normal nodes, and it is constant in this paper.

(2) T denotes the time that m_{i3} is blocked, and it can be controlled by the attacker.

Therefore, in the time of T, the probability that m_{i4} transmits RTS to m_{i3} is

$$P_1 = \int_0^T \frac{2(1-2p)}{(1-2p)(W+1)+pW(1-(2p)^m)}dt \quad (0 < t < T) \tag{2}$$

Suppose there are r chains which would be established in the cluster network, and all nodes accord with the distance requirements of the condition (1), the probability that the attacker makes its neighboring nodes to be blocked and the blocking problem propagate throughout the whole network is

$$P = (\int_0^T \frac{2(1-2p)}{(1-2p)(W+1)+pW(1-(2p)^m)}dt) \times (\int_0^{T'} \frac{2(1-2p)}{(1-2p)(W+1)+pW(1-(2p)^m)}dt)^{r-1} \tag{3}$$

The cluster network model used in this paper is seen in Figure 3, and n=14, there are three pairs of data links except that a pair of attackers, i.e. r=3. According the formula (3), if p, n, and r are certain, P is decided by three parameters of the network, i.e. the maximum backoff stage m, the minimum backoff window W, and the time T that m_{i3} is blocked. And T is bigger, W is smaller, so P is bigger and the attack effect is more obvious.

4. Defense strategies

The essential of the blocking attack, which utilize the structured characteristics of the cluster and the flaws in the RTS/CTS mechanism, is to reset the NAV of normal nodes by the exchange of spurious RTS/CTS, If the value of NAV is not zero, the nodes will not work, which is equal to be blocked. Then attackers utilize the time difference of the backoff mechanism to propagate the blocking problem throughout the whole cluster. Therefore, to defense this attack, it is very important to monitor the duration field in the RTS/CTS frame.

Based on above analysis, the defense strategy of duration field validation is proposed. The concrete method is described as follows. After each node in the network overhears a RTS or CTS frame on the MAC layer, it first caches the value of the duration in the frame, and then estimate the time that the transmission would occupy the channel actually according to the other following frames, and compares it with the former cache value. If they are not consistent, the node will be considered as an attacker.

For example, in NS-2.33, the values of various duration in RTS, CTS, DATA, and ACK respectively are rf_duration, cf_duration, dh_duration and af_duration. Because dataRate_= 11Mb and basicRate_= 1Mb, for the data frame with certain length, its transmission time is certain. In addition, the frame lengths of RTS, CTS, and ACK are respectively 20bit, 14bit and 14bit, and the value of SIFS is 10 μs, so only the length of DATA frame is a variable. If a node receives a RTS frame, it first caches the rf_duration, and then estimate the actually value of rf_duration according to the received DATA frame, which is denoted as rf_duration′. The computation formula is

rf_duration′=usec(3×phymib_.getSIFS()+txtime(phymib_.getCTSlen(),basicRate_)+txtime(pktTx_)+txtime(phymib_.getACKlen(),basicRate_))

If rf_duration′ and rf_duration are not same, or the DATA frame is not received, the sender of RTS is considered as an attacker. Then the attackers' information will be broadcasted to other nodes, and the attacker will be insulated from the network.

5. Simulation analysis

The simulation platform is windows xp and cygwin+NS-2.33. The blocking attack and the defense strategies are all simulated based on this platform.

(1) Simulation of blocking attack

In the experiment, normal nodes all adopt IEEE802.11 DCF as the protocol of the MAC layer, and the movement range of the nodes is the square region of 1200m×1200m including 15 nodes, and the node model adopts the structure as seen in Figure 3, i.e. m_1 and m_2 are set to be a pair of attackers. Simulations using constant-bit-rate (CBR) sources, and the size of CBR is 512bit, and the rate is 10kb, and the simulation time is 200s. To compare, the experiment compiles two scripts, and one has not attacker, and the other has a pair of attackers, and its MAC layer follows the MAC protocol with attacking behavior (adding before simulation).

The value of duration in the RTS frame exchanged by attackers is set to be 32767 μs, and the value of the competition window CW is set to be 1/2 of the normal node. Then by analyzing the trace files, we statistics the throughputs before and after the network is attacked, and draw them by the gnuplot. The descending of throughput is seen in Figure 5, and the result shows that the average throughput descends for 65.8%.

(2) Simulation of defense strategies

For the same simulation model and parameters of blocking attack, we add the defense strategy of duration field validation described above, and make the further experiment. The statistical result about the improvement in network throughput is seen in Figure 6, and the decrease of the throughput is 13.1% of the throughput without attack, and it is obvious that the decrease of the throughput is improved largely.

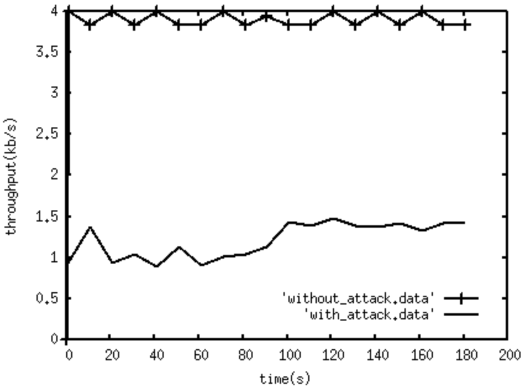

Figure 5. Throughput Change With the Attack

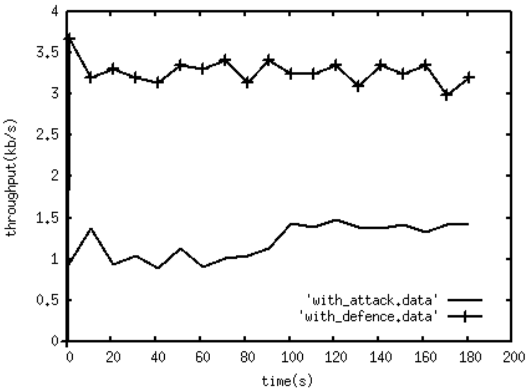

Figure 6. Throughput Change With Defense Strategies

6. Conclusions

The environment of the battlefield self-organizing network is particular, and the security mechanism is not mature enough, facing many security problems, for example, the Virtual Carrier Sense mechanism would makes it suffer many DOS attacks , and the blocking attack that a pair of attackers block the members in the cluster also belongs to it. The blocking attack is the result of attackers make use of the characteristics of the cluster structure and the flaws of RTS/CTS mechanism. This paper uses the NS-2.33 simulation software to test the blocking attack and the defense strategy, and statistics the network throughput. The result indicates that the blocking attack would obviously reduce the network throughput, and this situation would be largely improved after the defense strategy of adding the duration field validation is applied.

References

A Rachedi, A Benslimane. (2008). Smart Attacks based on Control Packets vulnerabilities with IEEE 802.11 MAC. *In Wireless Communications and Mobile Computing Conference.* P.588-593.

B Wu, J Chen, J Wu, et al. (2007). A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. *Wireless Network Security,Springer.* No.17. P.103-135.

CHEN Wei, YU Lei, ZHANG Ying-zhou. (2008). Vulnerabilities analysis of RTS/CTS mechanism in 802.11 protocols. *Computer Applications.* No.28(12). P.3183-3186.

D Chen, J Deng and P K Varshney. (2003). Protecting Wireless Networks against a Denial of Service Attack Based on Virtual Jamming. *In the Ninth ACM Annual International Conference on Mobile Computing and networking (MobiCom) Poster, San Diego.* P.14-19.

G Binachi. (2000). Performance Analysis of the IEEE 802.11 Distributed coordination function. *IEEE Journal on Selected Areas in Communications.* No.18(3). P.35-547.

J Deng, Z Zhang, S Pagadala, et al. (2005). Protecting MANETs from Spurious CTS Attacks with Randomized Carrier Sensing. *IEEE Sarnoff Symposium.* P.27-31.

K Bian, J Park, and R Chen. (2006). Stasis Trap: Cross-Layer Stealthy Attacks in Wireless Ad Hoc Networks. *In the IEEE GLOBECOM.* P.1-5.

K Xu, M Gerla, S Bae. (2003). Effectiveness of RTS/CTS handshake in IEEE 802.11 based ad hoc networks. *Ad Hoc Networks.* No.1(1). P.107-123.

Lei Guang, Chadi Assi. (2005). Vulnerabilities of Ad Hoc Network Routing Protocols to MAC Misbehavior. In IEEE WiMob. P.146-153.

S Djahel, F Nait-Abdesselam and F Ahsan. (2009). Highlighting the Effects of joint MAC Layer Misbehavior and Virtual Link Attack in Wireless Ad Hoc Networks. *In AICCSA,.* P.756-763.

S Ray, D Starobinski. (2007). On False Blocking in RTS/CTS-based Multi-hop Wireless Networks. *IEEE Transactions on Vehicular Technology.* No.56(2). P.849-862.

S Ray, J B Carruthers and D Starobinski. (2003). RTS/CTS- Induced Congestion in Ad Hoc Wireless LANs. *In IEEE Wireless Communication and Networking Conference (WCNC), New Orleans.* P.1516-1521.