Wireless Pers Commun (2013) 69:623–638
DOI 10.1007/s11277-012-0593-7

Protecting Satellite Systems from Disassociation DoS Attacks

Ting Ma · Yee Hui Lee · Maode Ma

Published online: 30 March 2012

Abstract With the help of satellites, the entire surface of the world can be covered, which provides the high speedy communications all over the world. Consequently, security is becoming an important concern in the satellite multicast communications. However, due to the inherent dynamic broadcast nature of the communication medium, this multicast system is easily susceptible to interferences and interceptions. In addition, the satellite system generally has a large number of terminal members with the high frequent join-leave characteristic. Therefore, the satellite systems face significant security challenges. The denial of service (DoS) is one of the most harmful attacks to the satellite systems and also terrestrial fixed or mobile networks. It can maliciously prevent legitimate users from accessing the service. It is especially true for the disassociation DoS attacks where an attacker sends bogus disassociation requests to disable the communication between the server and their legitimate clients. In this paper, the main focus of our work is to detect and defend against the disassociation DoS attacks on the satellite system. We also provide preliminary modeling verifications and simulation results regarding the efficiency and practicability of this new approach. Further analysis of the proposed method is also appended to demonstrate its feasibility.

Keywords Satellite system · Denial of service (DoS) · Disassociation · Sequence number

T. Ma · Y. H. Lee · M. Ma (✉)
School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, Singapore
e-mail: emdma@ntu.edu.sg

T. Ma
e-mail: mati0004@ntu.edu.sg

Y. H. Lee
e-mail: eyhlee@ntu.edu.sg

1 Introduction

Since the coverage area of a satellite greatly exceeds that of a traditional terrestrial system, the satellite multicast applications now are playing an increasingly significant role in our daily life, such as telecommunications from remote locations, satellite-delivered high-definition television (HDTV), radio broadcasting services, and amateur communications as well [1]. However, due to its dynamic broadcast characteristic, satellite systems are subjected to many different kinds of threats and attacks [2]. One of the most pervasive attacks is the denial of service (DoS) attack. A DoS attack is to deliberate sending of bogus messages to the server with the aim of disrupting the satellite network communication service. Due to the limited resources offered by a satellite system, flooding spurious packets can highly exhaust the systems' limited energy, bandwidth, memory and CPU capability. Furthermore, some vicious adversaries can deliberately send spoofed disassociation requests to the server, resulting in an interruption to the communications between legitimate clients and the server.

The DoS attack is one of the most critical security issues of any wireless communication network. The literature is flooded with solutions for DoS attacks over the last few years [3–7].The DoS attacks problems related to the physical layer are in the form of jamming. The common defense technique against jamming of the physical-layer in the wireless networks is the spread-spectrum [8]. The MAC layer is also vulnerable to the DoS attacks, including collisions, interrogation, and packet replaying. The strong end-to-end authentication and anti-replaying are needed to protect the MAC layer against DoS attacks. For the network layer, efforts have been done to deal with security of routing protocol, in particular, spoofing, replaying or altering routing traffic. The TCP SYN flood attack at the transport layer aims at expending the connection buffer resources. The SYN cookies which encode information from the client's TCP SYN message are employed to protect transport layer from flooding attacks. And the application layer has security concerns with prevention, malicious nodes, and virus detection. Packet authentication and anti-replaying techniques are applied to preventing adversaries overwhelming networks.

Although there are many solutions that have been reported in the literature for protecting wireless networks against DoS attacks, they are not effective to be applied to satellite systems. The most distinct difference between wireless communication and satellite communication is the distance, which generates high latency. The propagation delay is expected to be the dominant element to the overall latency in the satellite system case. The end-to-end latency between two satellite terminals will be roughly 300 ms for GEO links [9]. Thus, the proposed solutions in literature cause additional delay would not be useful to the satellite system.

In order to prevent DoS attacks to satellite networks, a round-trip time (RTT) based prevention technique to secure satellite networks has been proposed in [10]. If the bandwidth consumption of the network increases and exceeds a pre-defined threshold, the monitor will consider it as a possible DoS attack. Once the DoS attack is detected, the monitor will send a test feedback to the client requiring it to decrease its sending rates to a specified value. If the transmission rate does not react within a single RTT, the attacker is deemed unresponsive and packets sent by the attacker will be discarded. Although this method does not require high computation cost as required by encryption, it is not a perfect defense technique against DoS attacks. This is because the RTT based technique depends on the difference between the value of bandwidth consumption and a pre-defined threshold value. Therefore, if the intruders launch a DoS attack and the bandwidth consumption does not exceed the pre-defined threshold value, the satellite system would not take any protective measures even though the whole system have indeed suffered from a DoS attack.

In [11], a protocol has been designed for preventing DoS attacks. It uses a two-step verification process to prevent DoS attacks. Firstly the sequence number retrieved from the message should be equal to a nonce value. Then, the monitoring system will compare the computed media access control (MAC) address value using its private key with the one retrieved from the message header for a match. Finally, the network control center (NCC) further verifies the integrity of the message. However, the sequence number of each message has not been protected by any information hiding technique. Hence messages are easily attacked by the DoS attacks.

In order to overcome the shortcoming of the solution in [11], in this paper, we propose an enhanced algorithm to protect the sequence number of each message. The proposed scheme evolves from the solution in [11]. Particularly, the Rabin function has been employed for the first step of the sequence number verification. The great advantage of the Rabin cryptosystem is that a random plaintext can be recovered entirely from the cipher text only if the code breaker is capable of efficiently factoring the public key. It has been proven that decoding the Rabin cryptosystem is equivalent to the integer factorization problem which is till now practically insoluble. The Rabin function can provide a strong protection to the sequence number, so that bogus packets can be identified instantaneously and then discarded. In contrast to previous works, the salient advantage of our scheme is its much stronger security functionality to prevent DoS attacks. It can effectively defend the satellite networks against DoS attacks simply by checking the value of the sequence numbers. By the analysis, it is demonstrated that the proposed scheme can achieve high performance in terms of detecting and preventing DoS attacks before any severe harm to the satellite networks happens.

The rest of this paper is structured as follows. In Sect. 2, an introduction to the satellite system model will be given together with a brief overview of the process of satellite communication. The detailed proposed scheme to prevent disassociation DoS attacks in the satellite system will be presented in Sect. 3. And then in Sects. 4 and 5, modeling verifications and security analysis of the proposed approach will be provided. Finally, a conclusion is given in the last section of this paper.

2 Satellite System Model

Standard digital video broadcasting-interaction channel for satellite distribution systems (DVB-ICSDS) [12] provides typical satellite system architecture as shown in Fig. 1. This satellite interactive network mainly comprises of the NCC and return channel satellite terminals (RCST). The functions of these two main components are:

NCC: A NCC is mainly responsible for the controlling and monitoring of functions. It generates the control and timing signals for managing the authentication and association of legitimate users in the satellite multicast interactive networks.

RCST: A RCST sends control messages such as connection requests to the NCC. These messages are transmitted via satellite using data transfer protocols.

In a satellite system, each RCST and NCC is assigned a unique MAC address. Every RCST shares a secret session key with the NCC which is pre-computed by the NCC. According to the public-key protocol, even if the intruder intercepts the MAC message, he cannot obtain the session key value. In addition, the NCC divides the time in fixed intervals T_i during which it reliably broadcasts a different nouce N_i for the purpose of replay detection. When a RCST registers in a satellite system, it will first perform negotiation handshaking with the NCC to establish authentication and confirm the cryptographic algorithms and the key size to be used subsequently. Once the negotiation step is completed, the NCC

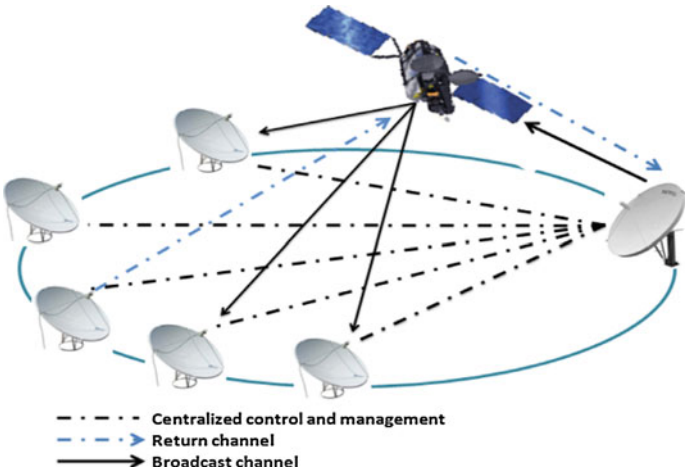

Fig. 1 Satellite system model

will proceed with the key exchange step by sending explicit key exchange (EKE) request messages.

The RCST replies to each EKE request message with an EKE response message, the NCC can authenticate the terminal based on the EKE respond message. Once the RCST receives verification from the NCC, the RCST is able to decrypt the encrypted data streams. Otherwise, the fake RCST will be detected. When some RCSTs want to disassociate with the NCC or when some new RCSTs want to associate with the NCC, the NCC needs to update the session key used in the satellite system. To transmit a new key, the NCC will send EKE request messages to each RCST.

The RCST will then extract the secret session key from the incoming EKE request messages and reply with an appropriate EKE response messages. However, this process is usually vulnerable to malicious attacks, especially, DoS attacks. DoS attacks maliciously prevent the legitimate clients from successfully accessing the system resources.

A DoS attack can be launched in a number of ways, the three basic types of attacks are:

(1) Consumption of limited resources, such as bandwidth.
(2) Disruption or alteration of configuration and state information.
(3) Destruction of physical network components.

The satellite system is a multicast system. Therefore, the process of multicast authentication, in particular the disassociation process, is susceptible to DoS attacks. The DoS attack targets at preventing communications from being forwarded properly.

3 Proposed Solution to Prevent DoS Attacks

In this paper, a disassociation DoS attack is our major concern. The operations of it have been depicted in Fig. 2. When there is a communication traffic flow between the NCC and the RCST via a satellite, adversaries who are listening out for the traffic can intercept the data messages. The intelligent adversaries can make use of these sniffed messages to generate a spurious disassociation request message. This dissociation message can either be sent by the RCST to the NCC or by the NCC to the RCST.

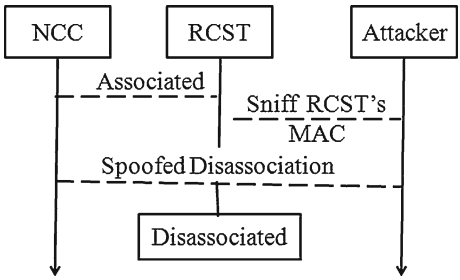

Fig. 2 A disassociation DoS attack

Once the NCC receives a disassociation request from the RCST, it will terminate its connection with this RCST and clear all stored states from its memory. If an intruder sends a bogus disassociation request to the NCC, the NCC will then terminate its communication with the victim RCST. If the victim RCST wants to access the service again, it has to go through the authentication process again. The authentication process not only involves the termination of the current normal data communication, but also requires more efforts and time to re-establish the authentication. Therefore, the bogus disassociation DoS has successfully consumed the systems' resources and disrupted the legitimate client communication with the satellite network.

Each message sent by a RCST has a unique sequence number [13]. Usually the sequence number is linearly distributed as $m_{i+1} = m_i + 1$. This sequence number can be used to detect if there are any packet loss in the communication process. However, if an intruder sniffs the sequence number, he can easily generate the next packet's sequence number by simply adding one to the current sequence number value and by spoofing the source MAC address using available tools such as Spoof-MAC [14], MAC Changer [15], and Airsnarf [16]. Then the malicious attackers are able to send a disassociation request to the NCC. The NCC may abort its service with the victim RCST, resulting in a disconnection between the RCST and the NCC. Furthermore, if the MAC address of the NCC is spoofed by some vicious intruders, then the intruders can send spurious disassociation requests to each RCST in the system. By so doing, the whole satellite multicast network system will then suffer destructive disassociation DoS attacks.

Given that the RCST checks the sequence number of a message at the first step to verify the incoming message, enhancement of security and reliability of this sequence number is necessary to prevent the disassociation DoS attacks. If a disassociation DoS attack can detect at the first step by simply checking the sequence numbers of the received message, then the cost of computation resources could be significantly reduce by avoiding the subsequent steps of MAC value and payload verification.

The basic idea of our proposed scheme is to employ the Rabin Function [17] over the sequence number instead of a plain sequence number. The Rabin function is a one-way function depicted in Fig. 3. Due to its property, if $y = R(x)$, the value of x cannot be determined given the value of y.

For the encryption, let $p = \{0, \ldots, n-1\}$ be the plain text. The encrypted text c is then given in (1) by

$$c = m^2 \bmod n \tag{1}$$

Where $n = p*q$, p and q are primes and $p = q \equiv 3 \bmod 4$.

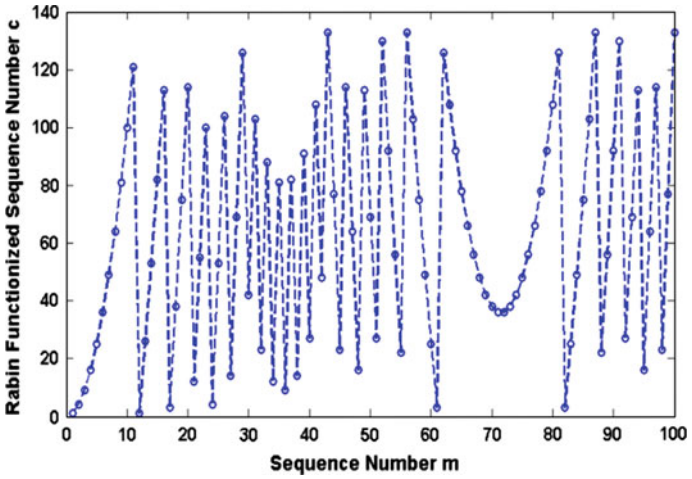

Fig. 3 Rabin function over sequence number

For the decryption, the p and q are necessary in order to obtain the value of m_p and m_q in (2).

$$\begin{cases} m_p = \sqrt{c} \bmod p \\ m_q = \sqrt{c} \bmod q \end{cases} \tag{2}$$

By applying the extended Euclidean algorithm, y_p and y_q, with $y_p * p + y_q * q = 1$, the values of y_p and y_q can be obtained. Next, by the invocation of the Chinese remainder theorem, the four square roots: $+r$, $-r$, $+s$ and $-s$ can be found in the set $\{0, \ldots, n-1\}$.

$$\begin{cases} r = \left(y_p \cdot p \cdot m_q + y_q \cdot q \cdot m_p\right) \bmod n \\ -r = n - r \\ s = \left(y_p \cdot p \cdot m_q - y_q \cdot q \cdot m_p\right) \bmod n \\ -s = n - s \end{cases} \tag{3}$$

Finally, with one of these square roots mod n, the original plain text value, m, can be obtained.

Based on the Rabin function, a lightweight scheme for authenticating the incoming packet by implementing protection onto its sequence number is developed.

3.1 Security Sign-on Session

When a session is being setup, one of three request/response MAC message-pairs is used to generate session keys specific to the payload streams associated with the session. A session key is a shared secret between the NCC and the RCST: even if every MAC message is intercepted, the cryptographic properties of the protocol ensure that an eavesdropper cannot determine the session key value. This is achieved by using a public-key protocol, which requires an up-front shared secret, or a simpler protocol based on a long-term shared secret between NCC and RCST called a cookie. The cookie is 160 bits long. It can be used by the NCC to authenticate the RCST log-on. Each RCST will store its own cookie in non-volatile storage, whereas the NCC will maintain a data-base of the cookie values of the RCSTs on its network. Cookie values will be updated occasionally as de-stated by security policy, but they are less vulnerable than session keys: a successful brute-force attack on a session key

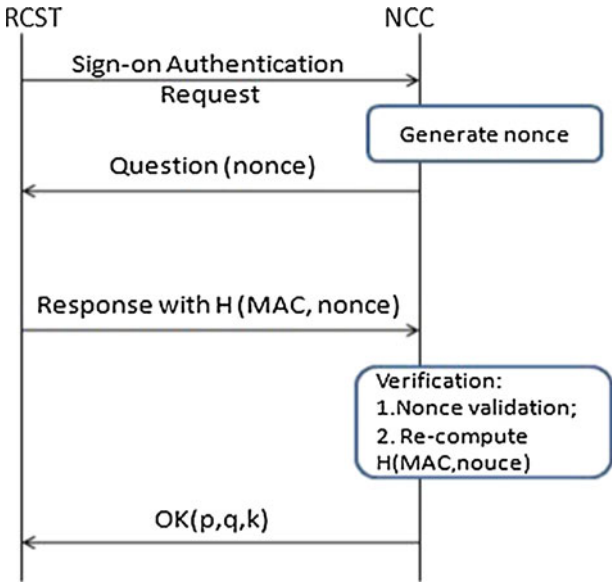

Fig. 4 ST sign-on authentication process with NCC

reveals nothing about the cookie value, nor any other session key. During the process of each ST logon, the ST and the NCC will authenticate each other through 4-way handshaking as illustrated in Fig. 4. This process is initiated by ST side when it requests for authentication to perform logon. Upon receiving a request, the NCC will send back a question that comprises a nonce which is a uniquely generated specific string. And then, the ST combines its MAC address and received nonce and responses to NCC using a mutually agreed hash function. The response is sent back to NCC for further verification. After receiving the reply, the NCC will firstly check the validation of the nonce and verify the user's identity checking its MAC address. If the recomputed response matches that retrieved from the received, the NCC will create a private session key as well as the corresponding p, q and k values with each ST. The private session key, p, q and k are shared secrets between the NCC and the ST. The sequence number of each sending message is encrypted and can only be decrypted by using the appropriate p, q and k values.

The basic verification process of an incoming message is shown in Fig. 5. Initially, after obtaining secret value p, q and k from NCC, the ST sends a message with the encrypted sequence number by using the Rabin function. ST will employ the encrypting process based on the prime numbers i.e. p and q which are chosen according to the value of k. With p fixed, if k is odd, q would be the kth prime number after the original q, whereas, when k is even, the q value would not be changed. We assume that NCC and ST mutually understand the effect of value k. Once the message from the ST is received, the NCC will decrypt the sequence number based on its p and q values. Due to the characteristics of the Rabin function, there may be several candidates of plain sequence number m. Therefore, the NCC needs to look up its sequence number table to find the right sequence number. If the decrypted sequence number is equal to the nonce N_i, then the NCC would go on to compute the value MAC $(K_{STi}, Seq|h(M))$ using the shared key K_{STi} that can be computed by K_{NCC}. Then, the NCC further verifies the value of the payload to ensure that it is equal to the value retrieved

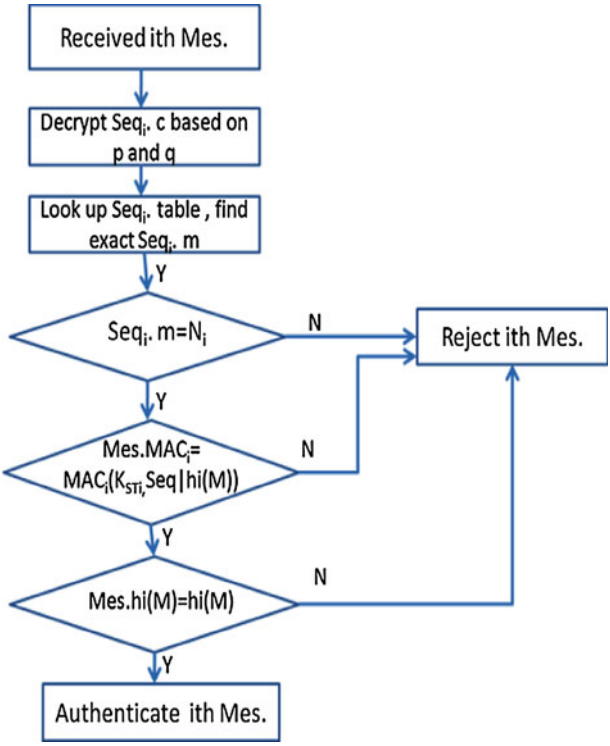

Fig. 5 Verification process of a received message

from the incoming message. All of the above steps have to be verified before the incoming message is accepted; else the NCC would discard the incoming message.

Our proposal is aimed to enhance the security protection of the sequence number of each request packet. It is achieved by encrypting the sequence number with the Rabin function. By use of one-way Rabin function to protect the sequence number, even if the attacker is able to sniff out the current sequence number, he will not be able to figure out the next exact right sequence number. Therefore, the NCC can discard the unauthorized attackers more quickly by avoiding following steps of verifications.

4 Modelling and Verification

Colored petri nets (CPN) has been adopted as the formal modeling tool for analyzing and verifying our solution. CPN is a graphical oriented language combining with the functional programming language standard ML for design, specification, simulation and verification of systems. It can support the expression of a greater range of interaction, and be used to establish model of concurrency for its intuitive graphical representation and relatively implementation. Besides, CPN-tools, which is a widespread tool for editing, simulating and analyzing CPN, can provide simulation of information flows dynamically and construct graphs automatically. CPN tools have strong formal definition for both its syntax and semantics, which provides a precise specification of the model generating, checking and simulation [18].

In this paper, we design three models based on CPN tools [19] to verify our solutions against Disassociation DoS attack. Given that our solution mainly strengthens security protection to sequence number, we will compare three different situations where general transmitting and receiving without attacks, existing disassociation DoS attacks without proposed solution and with solution to prevent DoS attacks in our CPN model.

4.1 CPN Model of Normal Communication Process

In CPN model, data is represented by tokens each belonging to a special data type called the color set of a token. The token color is the actual assignment of values to this token. Each color set which can be variable, constant or function has to be declared first as a new color set. To model the messages, two color sets SN and DIS are declared to be the sets of integers. Color set SN is defined to represent the sequence number of the transmission message, while color set DIS is declared for modeling the states of performing dissociation request.

The CPN model for the normal process of communication between NCC and ST is shown in Fig. 6. In order to intuitive demonstration significance of protection on sequence number, we simply define each packet consisting of two parts which are sequence number and disassociation request state. When NCC receives a packet from ST, it will first check dis value with stateyes which is a constant defined as one. In this model design, if the value of variable dis is zero, we consider it as a sign of disassociation request. In this case, NCC will accept its request and abort communication with ST. But if there is no request for disassociation, NCC will go on to check its sequence number of incoming packet with its next sequence number list. If sequence number is consist with the one in NCC's NextSn list, and then NCC side will send an acknowledgement to ST. Hence it is general model of communication between NCC and ST without attacks.

4.2 Disassociation DoS Attacks

In the scenario when intruder want to interrupt the communication between legitimated client and NCC side, intruder will eavesdropping on the traffic and obtain the sequence number that is being transmitted from ST to NCC. Since unencrypted sequence number is sequential, it is easily for the intruder to generate fake sequence number just by adding one to current

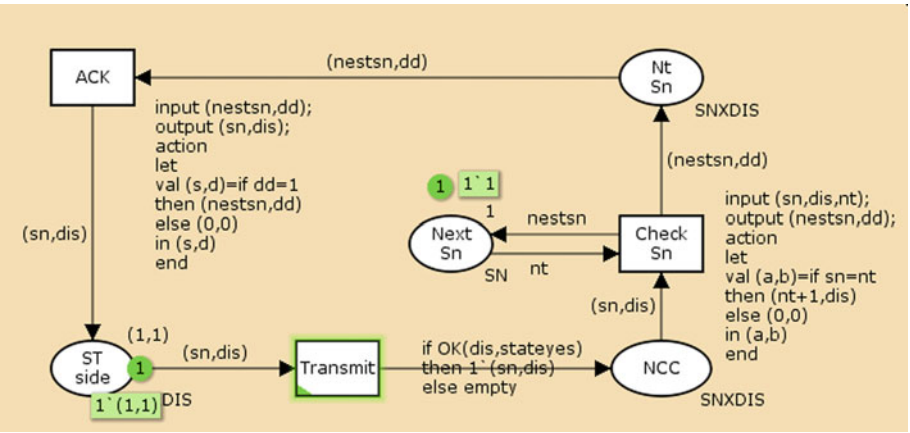

Fig. 6 CPN Model of normal transmission system

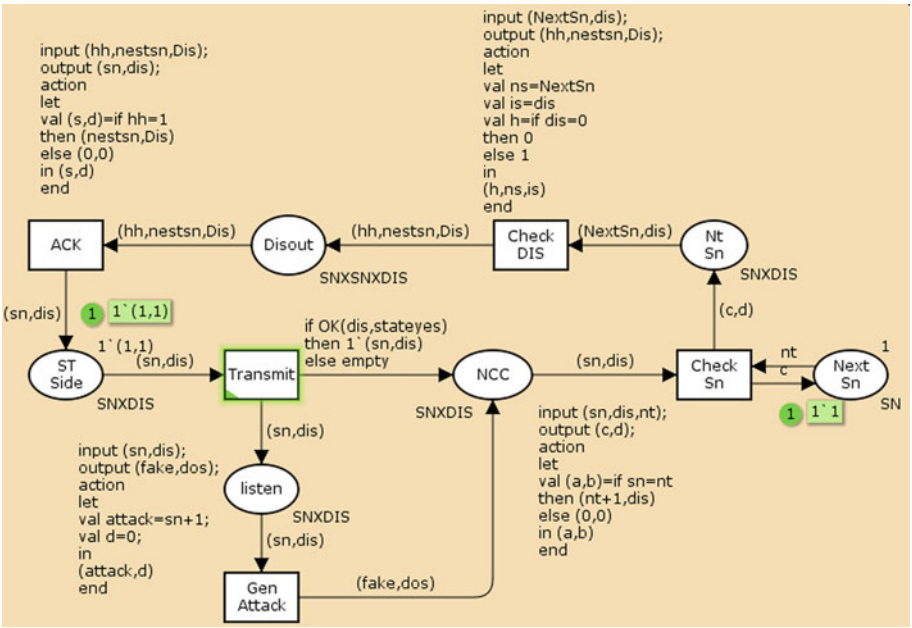

Fig. 7 CPN model of communications with disassociation DoS attacks

value of sequence number. Subsequently, intruder will send a fake dissociation request with its stolen sequence number. In this paper, in order to analyze significance of encryption to sequence number, we suppose intruder can get right verifications of its MAC address and payload during subsequent steps. Hence, if the intruder could eavesdrop on sequence number, he could make a disassociation DoS attacks which makes true client could not access NCC anymore.

Similarly, we use CPN to conduct the process of this kind of disassociation DoS attacks as depicted in Fig. 7. In this model, place ST Side represented as ST is responsible for sending packets to place NCC. At the same time, the attacker also listens on the transmission traffic and generates flooding disassociation DoS attacks to the place NCC. Since the potential attackers set dis to zero and send it to NCC with correct next sequence number, the NCC would accept it and take it for the disassociation request from legitimated users. Consequently, the ST side could not communicate with NCC smoothly due to the successful interruption by the malicious intruders.

4.3 Proposed Solution to Prevent Disassociation DoS Attacks

As previous descriptions of our proposed method, we conduct the CPN model to verify our scheme. Based on normal transmission CPN model, we develop it by adding encryption model, attacker side model, MAC check model and decryption model. Therefore, we can show the whole process in which malicious intruders attack the communication and be detected by our proposed solution through our simulation CPN model.

The encryption of sequence number model is shown in Fig. 8. The transmission message is defined as product of three color sets of SN, DIS and MAC. Firstly, the message from

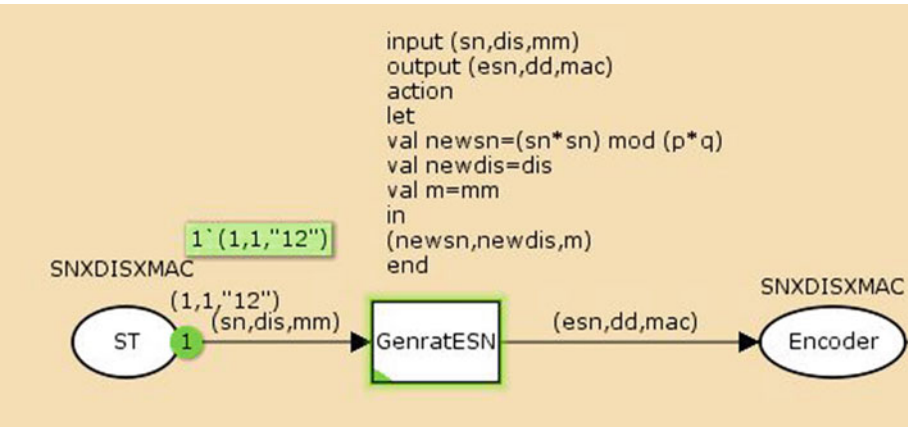

Fig. 8 Encryption to sequence number with Rabin function model

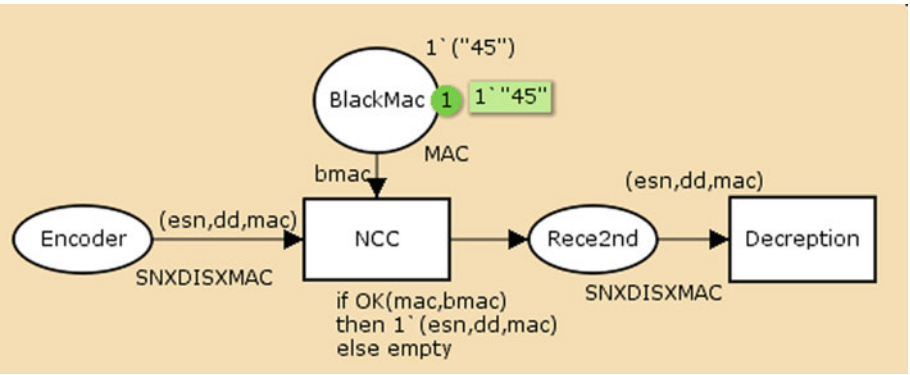

Fig. 9 The MAC check model

place ST is received by transition GenratESN. And then transition GenratESN conducts its function of employing Rabin function to encrypt sequence number of incoming message.

The attacker eavesdrops on the traffic model is the same as previous model two presented. In order to detect the intruder, we conduct MAC address check model that is depicted in Fig. 9. Hence, NCC side will firstly check MAC address of every incoming message before decryption part. In addition, if sequence number of transmission packet is not the same as the one stored in NCC's list, NCC will automatically consider it as malicious attacker and save its MAC address to its BlackMac place. If the attacker wants to send fake disassociation requests next time, it will be detected immediately by MAC check part of our solution. Therefore, we can prevent flooding DoS attacks in this way.

Lastly, after verification of MAC address, place NCC will move on to conduct decryption part model as demonstrated in Fig. 10. Resulting from decryption algorithms of Rabin function, there are four candidates for decrypted sequence number. The function of SelectSN transition is to compare decrypted sequence number with NextSn stored in NCC's list place. If one of four decrypted sequence numbers and NextSn are consistent matched, NCC will update its NextSn place and send an ACK to ST side. On the contrary, if decrypted sequence number is not corresponding to NextSn, NCC will treat current sender as an attacker and

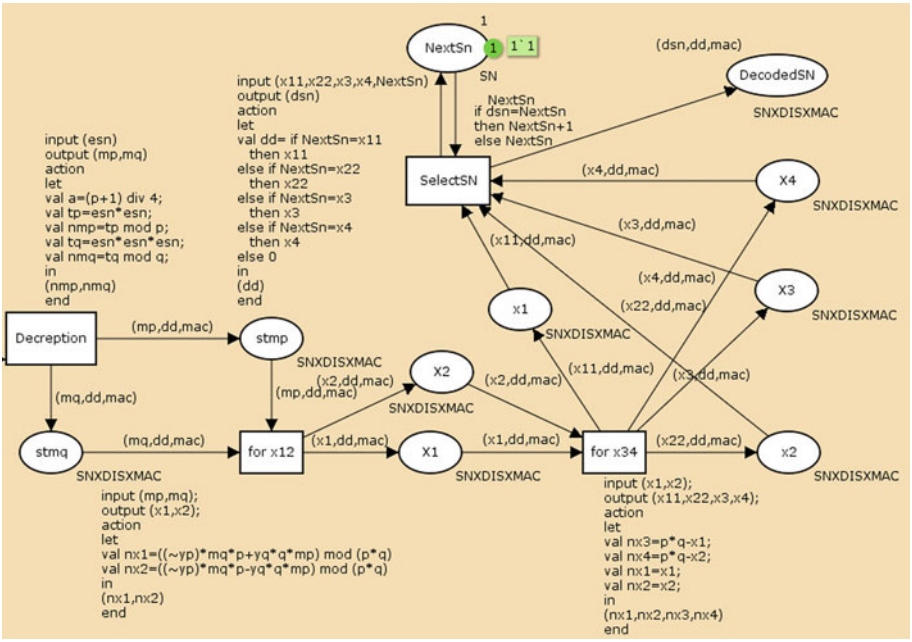

Fig. 10 The decryption of sequence number at NCC model

put its MAC address on the BlackMac place to prevent it from sending malicious request again.

5 Analysis of Proposed Solution

The proposed solution allows not only the quick detection of disassociation DoS attacks but also the prevention of disassociation DoS attacks. The attacker sniffs messages from the ST and creates a bogus message using a sequential sequence number. By our proposed solution, the NCC can easily distinguish the fake packets from the authorized packets, and the sequence number from the encryption of the sequence number by the Rabin function. Therefore, the NCC does not need to check its MAC and payload values, avoiding the cost of computation and resources.

In order to estimate the probability of successful disassociation DoS attack, a simulation has been conducted using MATLAB. It is assumed that an intruder successfully sniffs a message sent by the ST to the NCC, including its sequence number, the ST's MAC address and other confidential data. The malicious attacker will send a spurious disassociation request message to the NCC using the counterfeit sequence number. According to the proposed scheme, the success of such a disassociation DoS attack depends on the identification of the correct sequence number.

According to the algorithm, a successful attack will occur if and only if there exit two consecutive encrypted sequence numbers by the Rabin function corresponds to the two normal consecutive plain sequence numbers. The prime values of the Rabin function is defined as $p = 7, q = 11$ and the size of the plain text of the sequence number varies from 100 to 40,960. The probability of a successful disassociation DoS attack calculated by the simu-

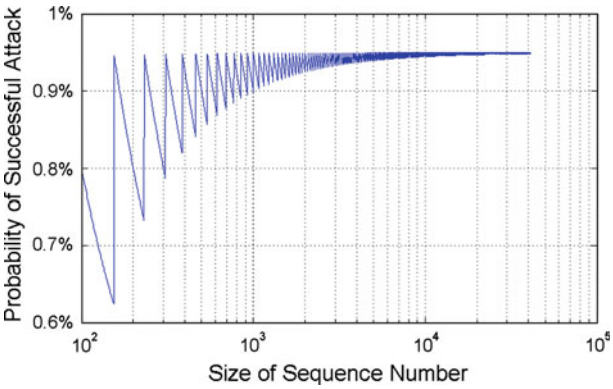

Fig. 11 Probability of successful attacks

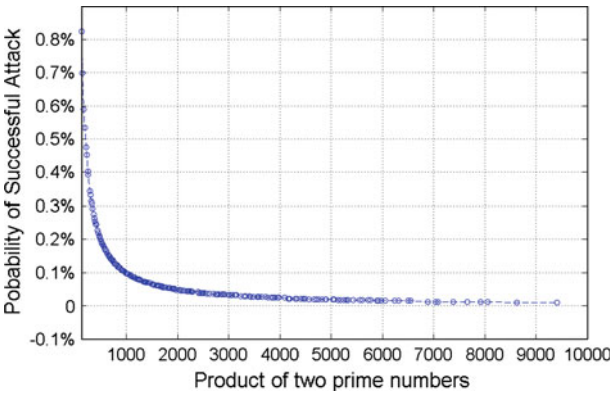

Fig. 12 Probability of successful attack versus products

lation is shown in Fig. 11. In this figure, it can be seen that the probability of a successful attack approaches a limit of 0.9 % along with the increase in size of the sequence number. It indicates that the risk of this solution can be controlled.

Furthermore, from the Rabin function, the products of the two prime numbers can affect the performance of the solution. Another simulation has been performed to study the effect of the product of the prime numbers on. the performance the performance The results are shown in Fig. 12. It can be clearly observed that the probability of a successful disassociation DoS attack approaches zero with the increase in the product of the two prime numbers. Thus it can be concluded that the larger the product of the two prime numbers, the lower the probability of a successful DoS attack. This indicates that the performance of the proposed solution can be enhanced by increasing the product of the two prime numbers p and q for the Rabin function. In conclusion, these results show that the proposed solution can achieve a good performance for the detection and prevention of disassociation DoS attacks to satellite multicast networks.

However, the previous analysis is based on the situation where the attackers cannot sniff the values of p and q to decrypt the cipher plain sequence number m of the Rabin function. In the situation where the attacker is able to obtain the values of p and q, then the attacker would be able to decrypt the encrypted sequence number c and obtain the plain sequence

number m. However, even though the attacker is able to obtain all the above information, due to the nature of the Rabin function, the decrypted numbers might have several candidate values. Therefore, the attacker is still unable to figure out the correct candidate value. At the NCC end, the redundant decrypted sequence number can be eliminated by comparing them with the latest received sequence number in its sequence number table. For example, if there are 4 numbers conforming to the Rabin function, the NCC can choose the one which is slightly greater than the latest received sequence number. By doing so, the probability of the attacker getting the right sequence number and makes a destructive attack on the satellite system will decrease much. In this sense the proposed solution can effectively detect and prevent disassociation DoS attacks.

6 Conclusion

The major contribution in this paper is to design a lightweight security scheme to detect and prevent disassociation DoS attacks to satellite networks. In such a disassociation DoS attack, the attacker can sniff the sending packet and generate a bogus disassociation request to the NCC, with aim to prevent legitimate users from accessing the service. Based on the characteristics of the one-way Rabin function, the proposed solution has employed the Rabin function to encrypt the sequence number in order to improve the security of the sequence number. Through the analysis of the simulation results, the proposed method is found to be able to efficiently prevent DoS attacks and have low consumption of computation resources by avoiding further verification. Future work would focus on the evaluation of the effectiveness of the proposed solution in more detail. Comparison of its performance with other methods will also be carried out.

References

1. Richharia, M., & Westbrook, L. D. (2010). *Satellite systems for personal applications: Concepts and technology* (1st ed.). London: Wiley.
2. Beaumont, J.-F., & Doucet, G., (2007). Threats and vulnerabilities of next generation satellite personal communications systems: A defense perspective. In *Globecom workshops, 2007 IEEE* (pp. 1–5). doi:10.1109/GLOCOMW.2007.4437787.
3. Micha, S., Michael, G., Car, A. G., Sanjeev, K., & Santosh, S. V. (2005). Mitigating DoS attack through selective bin verification. In *Secure network protocols, 1st IEEE ICNP workshop, 2005* (pp. 7–12).
4. Zhou, B., Marshall, A., Zhou, W., & Yang, K. (2008). A random packet destruction DoS attack for wireless networks. In *Communications ICC'08 IEEE international conference* (pp. 1658–1662).
5. Wang, L., & Srinivasan, B. (2010). Analysis and improvements over DoS attacks against IEEE 802.11i standard, networks security wireless communications and trusted computing. In *2010 second international conference* (pp. 109–113).
6. Kiuchi, T., Hori, Y., Hori, K., & Sakurai, K. (2010). A design of history based traffic filtering with probabilistic packet marking against DoS Attacks. In *2010 10th annual international symposium on applications and the internet* (pp. 261–264).
7. Sirikarn, P., Vasaka, V., & Panita, P. (2007) Lightweight detection of DoS attacks. In *Networks, ICON 2007 15th IEEE international conference* (pp. 77–82).
8. Chiang, J. T., & Hu, Y.-C. (2012). Cross-layer jamming detection and mitigation in wireless broadcast networks. *IEEE/ACM Transaction on Networking, 19*(1), 286–298.
9. Henderson, T. (1999) *Networking over next-generation satellite systems*. Ph.D. thesis, University of California at Berkeley.
10. Taleb, T., Kato N., & Nemoto, Y. (2004) A round-trip time-based prevention technique to secure LEO satellite networks from denial-of-service attacks. In *2004 IEEE 60th vehicular technology conference, 2004. VTC2004-Fall*, September 26–29, 2004 (Vol. 6, pp. 4012–4016).

11. Onen, M., & Molva, R. (2004). Denial of service prevention in satellite network. In *2004 IEEE international conference on communications*, June 20–24, 2004 (Vol. 7, pp. 4387–4391)
12. European Standard: ENSI EN 301 790 V1.5.1. (2009-05). *Digital video broadcasting; interaction channel for satellite distribution systems* (pp. 135–151).
13. Aslam, B., Islam, M. H., & Khan, S. A. (2006). Pseudo randomized sequence number based solution to 802.11 disassociation denial of service attack. In *Proceedings of the first mobile computing and wireless communication international conference. MCWC2006* (pp. 215–220). DOI:10.1109/MCWC.2006.4375224.
14. SpoofMAC. www.klcconsulting.net/smac/.
15. MAC Changer. www.alobbs.com/macchanger/.
16. Airsnarf. www.airsnarf.shmoo.com.
17. Buchmann, J., & Kaiser, M. (2007). *Computer proven correctness of the rabin public-key scheme* (Vol. 27). World Academy of Science, Engineering and Technology.
18. Ratzer, A., Wells, L., Lassen, H., Laursen, M., Qvortrup, J., Stissing, M., et al. (2003). *CPN tools for editing, simulating, and analyzing coloured petri nets, applications and theory of petri nets* (pp. 450–462).
19. CPN Tools. Homepage: http://wiki.daimi.au.dk/cptools/cpntools.wiki.

Author Biographies

Ting Ma received her B.E. degree from University of Electronic Science and Technology of China in 2009. Now she is working towards the Ph.D degree in Electrical and Electronics Engineering from the Nanyang Technological University. Her research interest is in security of satellite systems and video streaming.

Yee Hui Lee received the B.Eng. (Hons.) and M.Eng. degrees in electrical and electronics engineering from Nanyang Technological University, Singapore, in 1996 and 1998, respectively, and the Ph.D. degree from University of York, York, U.K., in 2002. Since July 2002, she has been an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University. Her interest is in channel characterization, rain propagation, antenna design, electromagnetic bandgap structures, and evolutionary techniques.

Maode Ma received his B.E. degree from Tsinghua University in 1982, his M.E. degree from Tianjin University in 1991 and his Ph.D. degree in computer science from Hong Kong University of Science and Technology in 1999. Now, Dr. Ma is a tenured Associate Professor in the School of Electrical and Electronic Engineering at Nanyang Technological University in Singapore. He has extensive research interests including wireless networking and wireless network security. He has led and/or participated in around 20 research projects funded by government, industry, military and universities in various countries. He has been a member of the technical program committees for more than 100 international conferences. He has been a general chair, technical symposium chair, tutorial chair, publication chair, publicity chair and session chair for more than 50 international conferences. Dr. Ma has more than 200 international academic publications including more than 70 journal papers, more than 130 conference papers and/or book chapters, and 3 academic books. Dr. Ma is the Editor-in-Chief of *International journal of Electronic Transport* and Topic Editor-in-Chief of *International Journal of the Advancements in Computing Technology*. He currently serves as an Associate Editor for *IEEE Communications Letters*, a Senior Editor for *IEEE Communications Surveys and Tutorials*, and an Associate Editor for International *Journal of Network and Computer Applications,* International Journal of *Security and Communication Networks,* and International Journal of *Wireless Communications and Mobile Computing*. Dr. Ma is a senior member of *IEEE Communication Society* and a member of a few technical committees in the *IEEE Communication Society.*