International Journal of Future Generation Communication and Networking
Vol. 9, No. 1 (2016), pp. 1-10

Random Tree Multicast Communications in Reconfigurable Network

Kaixiang Huang[a], Yue Chen[a,b], Julong Lan[a,b] and Hongyong Jia[a]

[a] *State Key Laboratory of Mathematical Engineering and Advanced Computing*
Zhengzhou, 450001, China
[b] *China National Digital Switching*
System Engineering and Technological Research Centre
Zhengzhou, 450002, China
kx.huang@outlook.com

Abstract

To increase the security of multicast, a Random Tree Multicast (RTM) scheme in reconfigurable network was presented. By decoupling data flow and group management, and by changing the multicast tree and channel with the technology of Moving Target Defense (MTD), RTM can improve the ability of defending eavesdrop and traffic analysis with little complexity. We present the details of our scheme, analyzed its performance, and discussed its advantages over traditional schemes.

Keywords*: Reconfigurable Network, Moving Target Defense, random tree multicast*

1. Introduction

The inflexible transport modes underlining today's network restricts the development of the networks. Its capability and structure are not well suited to the requirement of all sorts of emerging transmission services. Important service requirements such as quality, security, and extensibility are not well supported. The gap between service requirements and basic network capabilities becomes bigger. The population of the software defined network [1, 2] such as OpenFlow [1] 4] project reflects the pursuit in finding more reconfigurable networks. More and more efforts have been devoted to promoting software defined network (SDN) [5, 6].The FARI -"Flexible Architecture of Reconfigurable Infrastructure", Chinese national basic research project aims at solving above problems in current networks [7]. Multicast [8] is an efficient way of disseminating information to large groups of users, and plays a significant role in network services, such as video conference and the delivery of network control messages. Unfortunately, the traditional IP multicast protocols are very complex, because the router not only needs to transmit the data but also forward the control messages to get the group membership and the global network information [9]. The new network paradigm (SDN), by separating data plane and control plane, the logically centralizing controller can control the behavior of the entire network and the router only to forwarding data. To design a simple and scalable approach to multicast is a significant in the future network.

To improve the security of multicast, a typical approach is to encrypt group data traffic with the group encryption key. So the group key management has been studied extensively for over a decade (GKMP [10], Clique [11], and Iolus [12]). However, in the current multicast protocols, the paths and the channel of the multicast are mostly static. It provides a significant advantage for adversaries to eavesdrop and gather information of the multicast data, and illegal join the group and send data. The Moving Target Defense (MTD) techniques are the mechanism via changing system to prevent attacks [13]. For instance, through creating periodically alternative random configurations and services,

ISSN: 2233-7857 IJFGCN

MUTE [14] forces attackers to continuously chasing their target, deterring, and eliminating attacks without interrupting regular network traffic.

This paper proposes a random tree multicast (RTM) scheme for the reconfigurable networks. The basic idea of RTM is that the channel and the forward tree of the multicast will change randomly to defend against reconnaissance, eavesdrop and DoS attack in the whole multicast session. The main contributions of this paper can be summarized as two. First of all, we design a secure multicast scheme on the basis of FARI network: in the management plane, the multicast controller calculates the multicast tree, manages the group, and informs the control plane; the control plan is responsible for implement the strategy from the management plane; the data plane only need to forward the data. Secondly, we bring the Moving Target Defense techniques into multicast spanning tree construction algorithms and the channel chancing algorithms, which improves the security of the multicast traffic by changing the multicast tree with the non-fixed periodically change of the channel.

The rest of the paper is organized as follows: Sec 2 presents related works, Sec 3 discusses the technique scheme for RTM, Sec 4 shows the evaluation results, and Sec 5 concludes the work.

2. Related Works

The development of the future network has become a global focus. It is urgent to research and explore key technologies suitable for future network application and innovation. Many researchers have already focused on the multicast transmissions based on the future network. For example, Andrzej [15] proposed a novel flexible packet forwarding method designed for future internet networks. This method allows for flexible routing path selection, enables seamless multi-path and multicast routing at the inter-domain level.

SDN is the key technology for the future networks. More and more multicast approaches based on SDN have been put forward. Bondan. [16] proposed a clean-slate approach called Multiflow for multimedia multicasting, and implemented the prototype using OpenFlow [17] technology. During the session of a multicast group, with logically centralized, this approach has realized the calculation of the best existing route between the source and client hosts, with the objective of reducing at maximum the delay with the processing of multicast events. Aiming to reduce event delay, Cesar. [18] also proposed a clean-slate approach called CastFlow, which anticipates processing for all routes from each possible source. To improve the robust, load balanced and adaptive of the video multicast, Lee el al. [19] designed an algorithms to compute multipath multicast in SDN. To address the multicast scalability problem in SDN, Huang. [20] proposed a multicast tree called Branch-aware Steiner tree.

Most of the existing works use the group key management to provide security of multicast communication. For example, Omar. [21] introduced an efficient scalable batch-rekeying scheme based on multiple key trees. Li. [22] commended a group key scheme to safeguard multicast privacy for multicast communications in smart buildings of the smart grid. With the development of future networks, the security of multicast in the SDN has been paid more attention. When a new member wants to join a multicast group, the request will be forwarded to the control plane. So multicast can enable centralized admission control, policy enforcement and the group key management, thereby alleviating security concerns [23-27].

But the MTD can change aspects of the system to present attackers with a varying attack surface [28]. Qi. [29-32] proposed two novel proactive MTD in SDN based unicast, named Random Route Mutation (RRM) and Random Host Mutation (RHM). RRM can defend against reconnaissance, eavesdrop and DoS attacks with changing randomly the route of multiple flows. RHM can thwart scanning and worm propagation by

transparently mutating IP addresses with high unpredictability and rate. Just like the idea of MTD that prevents the malicious hosts from tracing and joining the group, Chen. [33] suggested a multicast scheme by changing the group address in the SSM channel at non-fixed periods. Though this solution is presented in IP network, it could also give us some enlightenment for improving the security of the multicast in SDN.

3. Random Tree Multicast Scheme with the Reconfigurable Networks

3.1. Architecture

The objectives of our scheme are (1) to ensure the integrity of the multicast session: even though the address and forwarding tree of the group are changing with non-fixed periods, a whole multicast session should not be interrupted; and (2) to strengthen the security of the multicast session: the rules of the changing should be hard to know for illegal users, so the multicast communication channel can be hided.

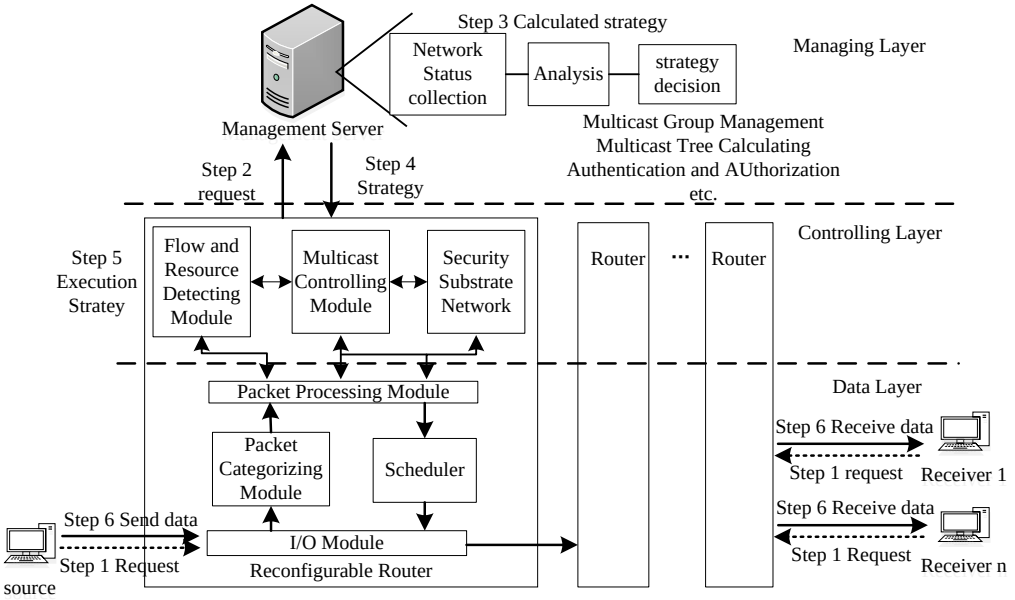


Figure 1. Multicast Architecture Based on Reconfigurable Network

Figure 1 illustrates the complete multicast communication process, which is divided into seven steps.

1) The source and receives will send the request packets (e.g. Internet Group Management protocol, IGMP [34]) to join or quit the group (S, E), where S is the address of the source s, and E is the destination address.
2) The packets will be forwarded to the management server by the reconfigurable router, which includes two layers. The data layer is only responsible for forwarding data. The controlling layer needs to route and implement security policies send by the managing layer, to detect the flow, topology and resources of network status, and to send status to the managing layer.
3) The management server belongs to the managing layer. It will compute the forwarding tree and the security policies (e.g. the key distribution and agreement) according to the network status and the group member. It can also adjust the tree and the policies dynamically.
4) The management server only sends the strategy to the reconfigurable routers which is on the path of the forwarding tree.

5) The reconfigurable routers will update the flow entries to the group (S, E_i).
6) While the source sends the data, the reconfigurable router forwards the data by the flow entry, and the receivers will get the data until the session finished.

When user leaves group or the network changes (e.g. some link loads are heavy.), management server will update multicast group memberships and change the path of tree updating the flow entries of routers.

3.2. Random Multicast Tree Algorithm

Obtaining the entire network topology, status, and all of the multicast group memberships, the management server needs to calculate multicast tree and the group channel with an algorithm which is called random multicast tree (RMT). Through establishing forward tree and assigning the multicast channel dynamically and randomly, attackers are hard to analyze traffic and obtain multicast transmission path. Once the attack is detected or a period is finished, the paths and channels will change, therefore the attackers need to attack again.

The network is usually modeled by a graph $G(V, E)$, where V is the set of nodes and E is the set of links. For each link $e \in E$, there are two parameters: available bandwidth b_{ij} and cost c_{ij}. A multicast session consists of the source node s and many receiver modes $g_i \in G$. We use a set of channels $(S, E_1), (S, E_2), ..., (S, E_n)$ and a set of trees $Tree_1, Tree_2, ..., Tree_n$ as a multicast session.

For a group multicast:

$$Minimize \sum_{k=1}^{n} \sum_{(i,j) \in T_k} c_{ij}, i \in V, j \in V \quad (1)$$

$$b_{ij} \geq B, (i, j) \in Tree \quad (2)$$

$$Time_i = Time_{i-1} + H_1(K_{(i-2) \bmod n}) \times (UP - DOWN) + DOWN \ , while, i = 1, Time_1 = Time_{start} \quad (3)$$

$$E_i = H_2(E_{i-1}, K_{(i-2) \bmod n}) \quad (4)$$

While, $Time_{start}$ is the start time when the source sends the traffic, E_1 is the initial group address of this multicast session, H_1 is a function that the value ranges between [0, 1]. One-way function H_2 and a set random key $K(0), K(1), ..., K(n-1)$ are used to generate frequency group address sequence. DOWN~UP is the range of the session cycle.

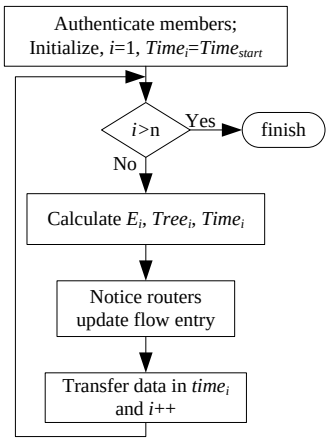


Figure 2. Flow Chart of Communication

The whole security multicast session is separated into three phases. Firstly, we confirm the legal multicast member via authentication. Secondly, we construct multicast tree according to the members. Thirdly, we change the tree and the channel at non-fixed periods. By using the random technology in the second step, it is difficult to obtain the multicast channel for attackers. Even if in some intervals, the attackers achieve to get the channel or some paths to get data, in the next interval they need to attack again. In the second step, we calculate E_i by Eq. (4), calculate $Time_i$ by Eq. (3). The tree of multicast should meet the goal (1) and the constraint (2). We extend the well-known Dijkstra's shortest path algorithm to consider both the load-balancing and multi-tree.

Random multicast Tree Algorithm

1: $Tree_0 = \{s\}$; $d[s] \leftarrow 0$; $d[g_i] \leftarrow \infty$; $Tree_{used} \leftarrow \varnothing$, for each $s \neq g_i$, $g_i \in V$

2: **insert** g_i with key $d[g_i]$ into queue *Q*, for each $g_i \in V$

3: **for** every $Time_i$

4: **while** ($Q \neq \varnothing$) **do**

5: $u \leftarrow Min(Q)$

6: for every node *v*, $v \notin Tree_i$ and *v* is adjacent to *u*

7: $alt = d[u] + ew(u, v)$

8: if $alt < d[v]$ then

9: $d[v] \leftarrow alt$

10: $pred[v] \leftarrow u$

11: add *v* into $Tree_i$

12: **End** $Tree = \{Tree_i\} + Tree$,

13: $Tree_{used} = \{Tree_{used}\} + \{Tree_{i-1}\}$

14: **End return** $Tree$

Figure 3. Random Multicast Tree Algorithm

The algorithm uses $d[g_i]$ to store the distance of the current shortest path form the source s to the node g_i , and $p[g_i]$ to store the previous preceding g_i on the current shortest path. The edge weight $ew[e]$ of *e* is defined according to Eq (5)

$$ew[e] = B / b_{(v,u)} + \alpha H_1(i) \; ; \; \alpha = \begin{cases} 1, & e \; in \; the \; Tree_{used} \\ 0, & else \end{cases} \quad (5)$$

Where H_1 is a function that the value ranges between [0, 1]. The algorithm uses α to store the edge e join in the $Tree_i$, to reduce the rate of choosing the edge e in $Tree_{i+1}$.

4. Evaluation

To study and demonstrate the feasibility of RTM, we use NS2 as the network generator for the evaluation. We use the Salama model to generate random topology with two parameters of Salama model as α=0.2, β=0.15. We assume that one sender will send 64B per 30ms and keep sending 600s, each router is connected with a receiver, and one controller is connected with all routers. When the routers get the message of JOIN(S, E_i), they will forward the message to the controller. The controller will ran the algorithm of RTM according to the topology and send the message of UPDATE(S, E_i) to each routers in the multicast tree.

4.1. Consumption Analysis

For a normal multicast, to maintain the multicast tree the number of messages (JOIN and UPDATE) is unchanged. In the FARI network, the controller will receive the JOIN messages, calculate the tree, and then send the UPDATE messages to the router. But, in the IP network, we can use PIM-SSM to find the multicast tree, which needs the messages to PRUNE and get multicast tree, therefore the messages will increase. In the scheme we presented, the number of control messages will increase with the changing times. For each analysis, we emulate 5 multicast sessions taking DOWN ~ UP respectively as 5 ~ 10, 10 ~ 15, 15 ~ 20, 20 ~ 25 and 25 ~ 30, and thus a session will take 600s. The number of the control messages is shown in Figure 4.

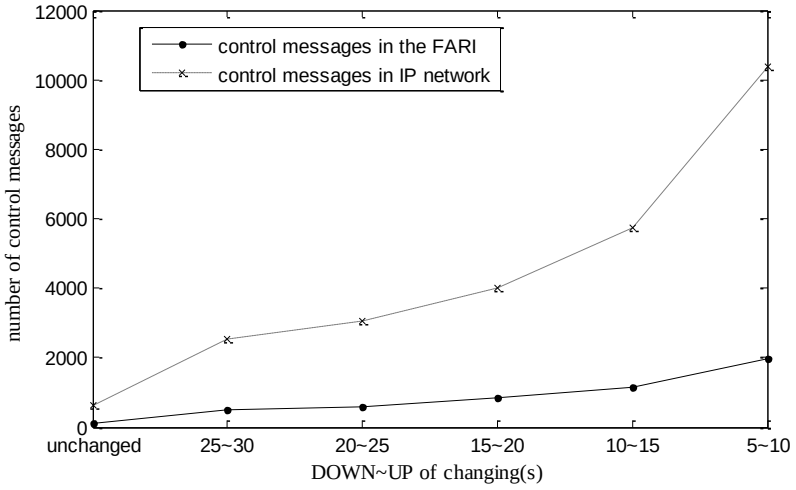


Figure 4. The Number of Control Messages Ranging along with Different Periods Changing Multicast

During each multicast session, we sum the state at every router for (S, E_i) per five seconds. After the session finishes, we use sum/(time*router number) to count the total state of (S, E) and the average of state at every router. It can be seen from table 1, that the multicast tree and channel change more frequency, and the overhead of control messages is more. But it's essential and worthy for the security. In the same topology, when the tree

and channel change in the FARI, it only needs to inform the new router to update the state. However, in the IP network (using PIM-SSM), the protocol should be used to find new tree, which needs lots of control messages. Table 1, also shows that the averages of state for (S, E_i) grow slowly. When the tree and channel do not change frequency, the number of state approaches 1.Therefore, there are only a little efficiency on lookup and data forwarding for multicast data packets.

Table 1. The Number of States According to Different Periods Changing Multicast

DOWN	UP	The sum of states	The average of states per router
5	10	11147	1.674
10	15	9272	1.387
15	20	8986	1.275
20	25	8475	1.189
25	30	8013	1.176
unchanged and in the FARI		7018	1
unchanged and using PIM-SSM		7018	1

4.2. Security Analysis

H_1 is a random function, which is used to calculate the transmission time for the next channel. It makes the time randomly changes among DOWN ~ UP. It also makes the channel changes without law. $K(0), K(1), ..., K(n-1)$ are random keys, which can ensure the security of channel hopping. H_2 is a one way function which is used to generate group address sequence. Thus, it's hard to deduce $K_{(i-2) \bmod n}$, even though the attacker obtains H_2 and $K(0), K(1), ..., K(n-1)$. Consequently, there is little chance to leak the key, and the initial key can be used repeatedly.

Besides, the multicast forwarding tree will change with the channel. During one channel (S, E_i), the attacker can get the data by attacking some paths or nodes of the tree. In our scheme, if the controlling layer detects the activities of attacks, it informs the managing layer to change the tree and channel from (S, E_i) to (S, E_{i+1}) immediately. Even the controlling layer does not detect the attack, during the channel (S, E_{i+1}) they must attack again. This costs the attackers more time and computation than only using the group key management. And we use H_1 to add the weight of the edge, and reduce the rate of the same edge appearing between two adjacent channels. In our scheme, the UP ~ DOWN is set as 5s ~ 30s, which can be adjusted according to the safety requirements.

4.3. Performance Analysis

To ensure the whole multicast session is not be interrupted, each router needs to keep the state some time for the channel (S, E_i). Even though the router receives the message of UPDATE (S, E_{i+1}), keeping the state a period of time that equals the maximum delay between *s* to *G* is also needed.

During each multicast session, the delay of the multicast session also changes with the tree. We emulate the multicast sessions with 9 members, and sum the delay time of every channel. After the session finishes, we use sum/time to count the average of delay time at every multicast session. Seen from table 2, the range of the delay time is acceptable.

Table 2. The Maximum Delay Time of Multicast Tree

DOWN	UP	The average of delay per multicast session (ms)
5	10	4.1
10	15	4.6
15	20	4.3
20	25	4.1
25	30	3.9
unchanged and in the FARI		3.6
unchanged in IP network		3.6

5. Conclusions

This paper presented a secure multicast mechanism using the MTD technology for FARI network, in which the channel and forward tree of the multicast could change randomly. Our mechanism enforces the ability of multicast to defend the malicious host receiving the multicast traffic, traffic analysis attack and the DoS attack. According to these experiments, our scheme will increase the cost of computational time and the control message, but it is worthwhile for the safety.

6. Acknowledgements

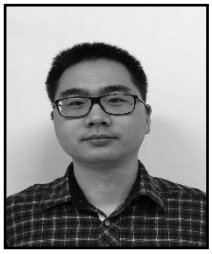
This work is sponsored by the National Basic Research Program of China (973 Program) under Grant NO. 2012CB315901. This work is also supported by National Natural Science Foundation of China（No. 61373006）.

7. References

[1] B.A. Nunes, M. Mendonca, X.N. Nguyen, K. Obraczka and T. Turletti, "A Survey of Software-Defined Networking: Past, Present and Future of Programmable Networks", Communications Surveys & Tutorials IEEE, vol. 16, no. 3, (**2014**), pp. 1617-1634.
[2] Open Networking Foundation, "SDN architecture overview", version 1.0, (**2013**).
[3] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner, "OpenFlow: enabling innovation in campus networks, ACM SIGCOMM Computer Communication Review", vol. 38, no. 2, (**2008**), April.
[4] A. Lara, A. Kolasani and B. Ramamurthy, "Network innovation using openflow: A survey", IEEE Communications Surveys and Tutorials, vol. 16, no. 1, **(2013)**, pp. 493−512.
[5] U.C. Kozat, G. Liang and K. Kökten, "On diagnosis of forwarding plane via static forwarding rules in software defined networks", In: Proc. of the IEEE INFOCOM, (**2014**).
[6] R. Cohen, L.L. Eytan, J.S. Naor and D. Raz, "On the effect of forwarding table size on SDN network utilization", In: Proc. of the IEEE INFOCOM, (**2014**).
[7] J.L, "LAN Research on the architecture of the reconfigurable fundamental Information communication network", Report of the National Basic Research Program of China (973 Program), (**2012**).
[8] S.E., "Deering Multicast Routing in Internetworks and Extended LANs", Proc. ACM SIGCOMM Symp. Comm. Architectures and Protocols, (**1988**), pp. 55-64.
[9] S. Keshav and S. Paul, "Centralized multicast, Network Protocols", (ICNP'99) Proceedings, Seventh International Conference on IEEE, (**1999**), pp. 59-68.
[10] H. Harney and C. Muckenhirn, "Group Key Management Protocol (GKMP) Architecture", RFC2094, (**1997**) July.
[11] M. Setiner, G. Taudil and M. Waidnet, "Cliques: A new approach to group key management", Technical Report RZ 2984, IBM Research, (**1997**) December.
[12] S. Mitta, "Iolus: A Framework for Scalable Secure Multicasting", In Proceedings of ACM SIGCOMM, (**1997**).
[13] J. Xu, P. Guo, M. Zhao, R.F. Erbacher, M. Zhu and P. Liu, "Comparing Different Moving Target Defense Techniques, Proceedings of the First ACM Workshop on Moving Target Defense", ACM, (**2014**).

[14] E. Al-Shaer, "Toward network configuration randomization for moving target defense, Moving Target Defense", Springer New York, (**2011**).
[15] A. Beben, P. Wisniewski, J.M. Batalla and G. Xilouris, "A scalable and flexible packet forwarding method for Future Internet networks", Global Communications Conference (GLOBECOM), (**2014**), pp. 1986-1992.
[16] L. Bondan, L.F. Müller and M. Kist, "Multiflow: Multicast clean-slate with anticipated route calculation on OpenFlow programmable networks", Journal of Applied Computing Research, vol. 2, no. 2, (**2013**), pp. 68-74.
[17] N. Mckeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Pererson, J. Rexford, S. Shenker and J. Turner, "OpenFlow: Enabling Innolvation in Campus Networks", In: ACM SIGCOMM COMPUTING COMMUNICATIONS REVIEW, Seatle, vol. 7, (**2008**), pp. 69-74.
[18] Teixeira and A.C. Ceasr, "CastFlow: Clean-slate multicast approach using in-advance path processing in programmable networks", Computers and Communications (ISCC), IEEE Symposium, vol.19, (**2012**), pp. 000094 – 000101.
[19] M.W. Lee, Y.S. Li, X. Huang, Y.R. Chen, T.F. Hou and C.H. Hsu, "Robust Multipath Multicast Routing Algorithms for Videos in Software-Defined Networks", Quality of Service (IWQoS), IEEE 22nd International Symposium, (**2014**), pp. 218-227.
[20] L.H. Huang, H.J. Hung and C.C. Lin, "Scalable Steiner tree for multicast communications in software-defined networking", arXiv preprint, (**2014**).
[21] O. Zakaria, A.H.A. Hashim and W.H. Hassan, "An Efficient Scalable Batch-Rekeying Scheme For Secure Multicast Co%%mmunication Using Multiple Logical Key Trees", IJCSNS, vol. 14, no. 11, (**2014**), pp. 35.
[22] D. Li, Z. Aung, S. Sampalli, J. Williams and A. Sanchez, "Privacy preservation scheme for multicast communications in smart buildings of the smart grid. Smart Grid and Renewable Energy", vol. 4, (**2013**), pp. 313-324.
[23] A. Iyer, P. Kumar and V. Mann, "Avalanche: Data center Multicast using software defined networking", Communication Systems and Networks (COMSNETS), Sixth International Conference, (**2014**), pp. 1-8.
[24] D. Kotani, K. Suzuki and H. Shimonishi, "A design and implementation of OpenFlow controller handling IP multicast with fast tree switchin", Applications and the Internet (SAINT), IEEE/IPSJ 12th International Symposium, (**2012**), pp. 60-67.
[25] J. Zou, G. Shou, Z. Guo and Y. Hu, "Design and implementation of secure multicast based on SDN", Broadband Network & Multimedia Technology (IC-BNMT), 5th IEEE International Conference, (**2013**), pp. 124-128.
[26] Y. Nakagawa, K. Hyoudou and T. Shimizu, "A management method of IP multicast in overlay networks using openflow", Proceedings of the first workshop on Hot topics in software defined networks, ACM, (**2012**), pp. 91-96.
[27] H. Li, P. Li and S. Guo, "Efficient privacy-preserving multicast in cloud data centers", Communications (ICC), IEEE International Conference, (**2014**), pp. 810-815.
[28] D. Evans, A. Nguyen-Tuong and J. Knight, "Effectiveness of moving target defenses, Moving Target Defense", Springer New York, (**2011**), pp. 29-48.
[29] Q. Duan, E. Al-Shaer and H. Jafarian, "Efficient random route mutation considering flow and network constraints", Communications and Network Security (CNS), IEEE Conference, (**2013**), pp. 260-268.
[30] H. Jafarian, E. Al-Shaer and Q. Duan, "Formal Approach for Route Agility against Persistent Attackers", Computer Security–ESORICS, Springer, (**2013**), pp. 237-254.
[31] E. Al-Shaer, Q. Duan and H. Jafarian, "Random Host Mutation for Moving Target Defense", Security and Privacy in Communication Networks, Springer, (**2013**), pp. 310-327.
[32] H. Jafarian, E. Al-Shaer and Q. Duan, "Openflow random host mutation: transparent moving target defense using software defined networking", Proceedings of the first workshop on Hot topics in software defined networks, ACM, (**2012**), pp. 127-132.
[33] Y. Chen, J.L. Lan, Y.T. Li and N. Wang, "Secure Source Specific Multicast Based on Channel Hopping", Computer Engineering, vol. 32, n0. 3, (**2006**), pp. 119-121.
[34] W.C. Fenner, "Internet group management protocol", vol. 2, (**1997**).

Authors



Kaixiang Huang, He received his M.S. degree in Computer Application from Institute of Zhengzhou Information Technology, a Zhengzhou, and is now a PhD candidate in computer application. He has worked in the area of broad band multicast. He is skilled in network security technology.

Hongyong Jia, He received his M.S. degree in Computer Application from Institute of Zhengzhou Information Technology, Zhengzhou, and his Ph.D. degree in Cryptography from Beijing University of Post and Telecommunication, Beijing. He has worked in the area of applied cryptography and network security. He is proficient in developing data packet authentication methods for the cloud and complex network environment.

Yue Chen, He received his M.S. degree in Computer Software from Institute of Zhengzhou Information Technology, Zhengzhou and his Ph.D. degree in Communication and Information System from China National Digital Switching System Engineering and Technological Research Centre, Zhenzhou. His research area broad band multicast. He is currently with network security technology.

Julong Lan, He received his M.S. degree in Communication and Electronic System from Xidian University and his Ph.D. degree in Communication and Information System from China National Digital Switching System Engineering and Technological Research Centre. He has worked in the areas of network router, parallel switch structure and IPv6 technology. He is currently the Chief Scientist in Chinese national basic research project- Flexible Architecture of Reconfigurable Infrastructure.