CL-004

Improving Security Problems in SDN-enabled Tactical Ad-hoc Network

Juhee Lee † Yasuhiro Nakamura ‡

1. Abstract

Today's tactical operations have complex communication and challenging requirements. Hence, merging Mobile ad-hoc network(MANET) and Software Defined Network(SDN) has been studied to facilitate highly configurable and robust network in the tactical environment. MANET provides robustness to overcome connecting failure against the restriction of radio coverage, and SDN provides high agility to control network. To make the best use of both technologies, most of the studies mainly focus on how to merging SDN and MANET. The purpose of this paper is to address security problems that could be occurred in SDN-enabled MANET and its countermeasures.

2. Introduction

If we look around, there are so many accidents happen such as fires, collapses, and sinking accidents, and earthquakes. And it is difficult to solve the problems by carrying out only one organization. This has led to a growing number of inter−organizational collaboration or multilateral operation. However, we cannot predict when and where those kinds of the accident would occurr, so that makes difficult to make communication during inter-organizational cooperation. Hence, numerous studies have been done to realize smooth communications with fixed infrastructures.

Network and computer-related technologies are developing from day by day, but in operational situations, requirements are too challenging to be fulfilled. And also, operational needs are postulate something remote from ordinary life, which makes operational needs more by more far from commercial requirements. Thus, a network system optimized for this operational situation is still under development.

2.1 The Operational Requirements

Operational requirements based on changing operational conditions are as follows:

1) **Flexibility**: In order to respond efficiently in this complex operational relationship and changing participants, there is a growing need for more flexible communicating systems. For example, path configuration under situational awareness is expected to have efficiency.
2) **Availability without fixed Infrastructure**: We cannot expect when or where we'll be conducting these operations above. Hence, a flexible communication system that can operate without fixed infrastructure is required.
3) **Interoperability**: There is also a growing need for joint operations, or coalition operations involving more than two units or countries. And there must be a group, who are using the equipment of heterogeneous specification. Therefore, interoperability is needed to actualize smooth communication between different groups.

† Graduate School of Science and Engineering, National Defense Academy
‡ Computer Science, National Defense Academy

2.2 Existing Measures

Up to date, Mobile Ad hoc Network(MANET) is applied to a tactical environment, so that a variety of information can be distributed without fixed infrastructure. Ad-hoc networks can be applied to various areas including emergency disaster situation and the military's tactical situation, as they can configure and maintain their own networks.

However, due to the unique features that Ad-hoc networks only have, the existing secure techniques used in traditional networks could not be applied as they were.[1] For this reason, the detection and management processing of node showing abnormal behavior was also burdensome, for the reason of it also becomes a division of roles between each node.

To solve these problems, several models have been proposed to make SDN-enabled MANET. SDN is a quite new and promising technology, being introduced recently. At first, it is difficult to find a point of intersection, but this paper will explain it in detail in the next section, Related Work.

3. Related Work

3.1 Mobile Ad hoc Network

Ad-hoc network environments are all nodes distributed and do not be supported by fixed infrastructure. Therefore, all nodes have to play a fair role to maintain autonomous network system. In addition, each node is mobile and used in a wireless way, allowing for a more flexible network than a wired network.

The Mobile Ad hoc Network is divided into several categories depending on its behavior. Typically, we classify MANET protocols into Table Driven (Proactive) and On Demand (Reactive) way. There are OLSR and DSDV as 'Table Driven' way, and AODV as the 'On Demand' way and DSR as well.

3.1.1 Limitations

There exist critical limitations in MANET system. Due to the unique characteristics of Ad-hoc networks alone, the security techniques used in traditional wired networks cannot be applied as they are.[1] Here is explanation of four limitations occurred in current MANET system.

First, in the Ad-hoc network, each node performs the functions of the host while performing the router's function.[1] In other words, internal and external security measures cannot be established for the router itself, as in a wired network.

Second, sharing of wireless channels allows both legitimate and malicious, non-legal nodes also can access wireless channels, making it easier for the network to be attacked.[1]

Third, because the resources of the nodes that make up the network are very limited compared to the wired network.[1] If there is a large amount of overhead due to the execution of the cryptographic mechanism or external attacks, then node might be excluded from the network.

Fourth, MANET protocols are not flexible enough to provide adaptive policies required for operation.[2] MANET is mainly focusing on decentralized architectures to achieve robust connections under the restriction of radio coverage.

3.2 Software Defined Network

3.2.1 SDN Concept

Software Defined Network(SDN) is regarded as one of the most promising technology. It has special concepts compared to conventional networks that we used to understood. The architecture of SDN is illustrated in Figure 1, which shows us the concept of it.

Separation of Control and Data Plane is the main concept in

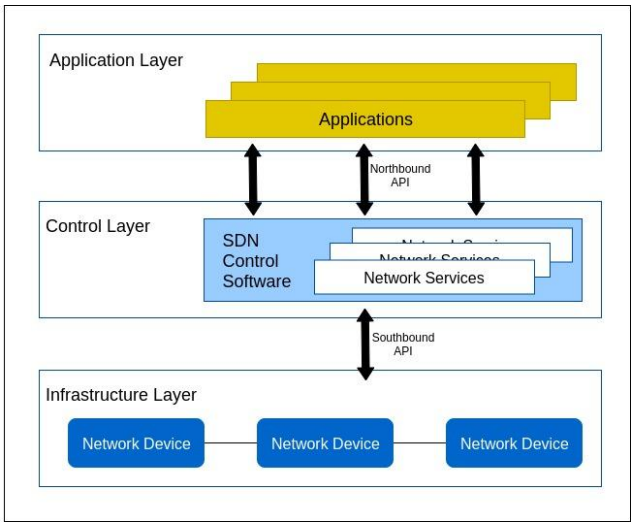

Fig. 1.SDN Architecture [5]

SDN. This made the control plane possible to be externalized from network devices, as “controller”.[7] The forwarding devices as data plane only process forwarding tasks. When forwarding devices have to process some tasks which they don’t have forwarding information, they just ask at control plane or forward these packets to control plane.

The controller is logically centralized. This means, it can be made up of multiple physical or virtual instances but acts like a single component. Physically multiple, but logically centralized controllers make network possible to get centralized control and survivability both.[7]

SDN provides an open interface to the outside that can define the functionality of network devices. This enables various network paths to be established, controlled, and managed with programmed software. Hence, SDN has a wide scope of potential in flexibility and adaptability.[7]

The external control plane and open interfaces enable SDN programmable. This is meaningful because it made possible to treat the network as a single programmable entity, instead of a set of devices that have to be handled individually.[7]

These kinds of new attributes of SDN show the potential to overcome MANET’s remaining restrictions.

3.2.2 Apply SDN to MANET

SDN showed us in some degree of possibility to overcome MANET’s remaining limitations. Concretely, MANET can be expected to be complemented by SDN in these following respects.

First, SDN provides enhanced management skills. It might be helpful to nodes to aware of their or neighbor node’s current state. Second, SDN is configured with open interfaces. This might be the key to solve communication problems between homogeneous groups. Third, dynamic policy application is possible to solve security problems.[4] SDN can be reactive depends on the state information of the nodes. Existing routing protocols(e.g. OLSR) are mostly focusing on path configuration, but SDN might provide plenty of state information without much overhead.

3.2.3 Limitations

Although we are expecting to make SDN-enabled MANET with a bright prospect, there also some restrictions still exist. First, applying SDN to wireless networks has just been discussed. It found quite optimal ways in wired situations, but still lack of consideration in wireless conditions. Second, in SDN, every operation presupposes that controller and forwarding have stable connectivity. So there are few alternatives to cope with the disconnection between data and control plane. Third, the protocol between controller and data plane, OpenFlow, generate considerable overhead to be used in wireless conditions. For those reasons, some situation cannot show SDN’s ability to the fullest. And we have to care about improving efficiency as the next research subject.

3.3 SDN-enabled MANET

SDN and MANET are conceptually different, so they have totally different orientations. Inherently, MANET aims for autonomous network configuration without central control. On the other hand, SDN aims at configuring centralization of the entire networks. But what tactical operations require is may completely autonomy in infrastructure configuration, not a complete autonomous system which does not follow central directives from the top. Therefore, a number of models of SDN-enabled MANET are proposed that adequately complement the shortcomings between SDN and MANET.

3.3.1 SDN-enabled MANET Models

When we are trying to configure SDN-enabled MANET, two questions inevitably have to be considered. The first question is where to locate the control plane, and how to use them. A second question is how to make forwarding devices to autonomously react to network changes while preserving the advantages of centralized control.[3]

The following are the distinctions of the model depending on where to place the controller. First, the controllers can be placed in several locations such as the command and control centers. Second, the controller can be configured in portable wireless infrastructure. Third, the controller could be deployed in the member’s equipment.[3] These models have their own strength and weakness according to the scale of the members or the

available resources depending on base equipment. For example, when the command and control center's controller tries to manage all of the nodes, it could generate considerable delays. Of course, this is depending on the scale of team members, but it is clear that it has a positive correlation.

The models classified according to the role distribution are as follows. This classification is proposed from [6], and models are considering further coalition operation's intrinsic situation.[6] First, centralized SDN controller, second, a hierarchical SDN controller, and last, a Federated SDN controller. When we need to conduct coalition operations with the team of another country, we cannot help reorganizing communication system to interact with each other. The centralized controller is very simple to organize, but lacks flexibility and raises a single point of failure. That's the reason why the Hierarchical model and Federated model is proposed. But, in this paper, we do not consider this aspect in detail.

There were also some models proposed by an idea that "How to maintain autonomy".[3] proposed a SMANET model which utilizes SDN as the main protocol and OLSR as sub-protocol. This can make use of SDN's merit as much as possible, but promptly change its protocol to be autonomous, when they cannot use SDN. [8] introduces a model that the SDN controller is connected with forwarding devices with "multi-hop" channel. This makes nodes to do not lost the function as a forwarding device. For this reason, it makes nodes to configure autonomous connection finally, even if additional hops are needed.

3.3.2 SDN-enabled MANET limitation so far

The performance of SDN-enabled MANET is still under researching, so there's not enough data that we can compare. But some methodological researches have actively been studied. Among the above models, only [8] simulated their SN enabled MANET models in NS-3 and estimated the performance of routing protocol.[8] enumerated the packets delivery ratio, throughputs, latency of SDN-enabled MANET compare to OLSR.

3.3.3 The purpose of this paper

In previous studies, security is not considered in previous studies even in a methodological way. The purpose of this research is to propose security-related performance evaluation standards, then to make SDN-enabled MANET models with a slight reference to the above studies. And then, progress research experiments on SDN-enabled MANET model, and then propose the optimal model which is suitable for the operational situation.

4. System Design

4.1 SDN-enabled MANET

In this paper, a single controller is deployed in the system. A blueprint of SDN-enabled MANET is illustrated in Figure 2.

1) The SDNC is hosted as a centralized controller.
2) The routing function is implemented as an application inside the SDNC and it is responsible for selecting the network.
3) The SDNC continuously collects the connectivity information from all the nodes and learns the network topology.[8]
4) All nodes are mobile and act both as forwarding devices and end hosts. They have limited wireless transmission ranges, so both the control and the data communications take place over multi-hop routes.[8]
5) The connectivity between SDNC and forwarding device is postulated as stable.

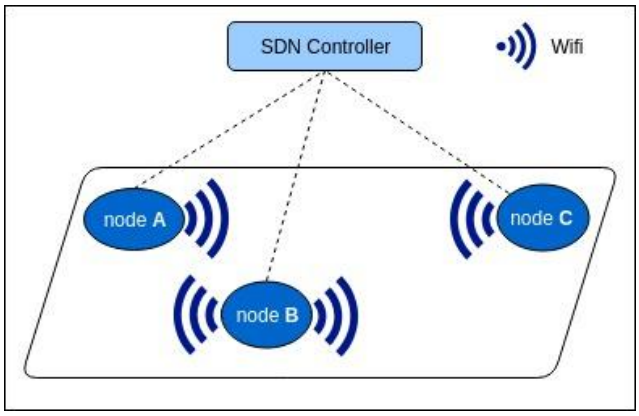

Fig. 2 System Design of SDN enabled MANET

4.2 Security Consideration

4.2.1 What is the most effective path, indeed?

When the topology changed, the nodes of MANET(e.g. OLSR) forward updated the information to their neighbors. And then, a new path is configured according to its algorism. But it cannot consider the node's state information in detail. It means, for example, even a node have only 1% of battery, it could be selected as the best way point of the entire path. It could be possible to apply battery information to existing algorism obstinately, as an additional parameter. But this is not the end. Maybe some of the links are very congested to use. We cannot apply all of the parameters in these ways, even if it is needed, because it will trigger a drastic amount of delay. We expect SDN-enabled MANET model is expected to solve this problem in a smarter way.

1) Simulate a node to have a lack of battery power.
2) Simulate a link to be heavily congested.
3) Compare the behavior of MANET and SDN-enabled MANET system.
4) Compare the time of survival time of the network.

4.2.2 How to protect SDN-enabled MANET networks from abnormal nodes

In ordinary life, it may be strange to consider malignant node except cyber attack. But it could be occurred by electric problems, or real interference from attackers. When it comes to the operational situation, the possibility to be under attack goes high. The troublemaker node can generate needless packets and sends it to others, or just reject to reply to any nodes. In MANET scenario, it is hard to know what is happening, and difficult to judge whether it is an attack or not. And even after right judgment, it is hard to counteract. But in SDN-enabled MANET, we can add or apply rule easier than before, because there is a controller.

1) Simulate a node to behave abnormally.
2) Simulate a link to be under jamming attack.

3) Check how MANET based node can detour troublemaker.
4) Estimate the counterattack ability of OLSR based network.
5) Check how SDN-enabled MANET based node can reflect new policies to disconnect troublemaker node.
6) Estimate the counterattack ability of SDN-enabled MANET based network.

4.2.3 How to maintain networks when a critical problem occurred in the controller or connection between node and controller?

When we apply SDN to MANET, it is important to think about how to connect node and control plane. And then, we have to consider how to counteract after this situation.

1) Simulate SDN-enabled MANET controller breakdown situation.
2) Simulate disconnection between controller and nodes.
3) Estimate the time to be changed into another plan.

5. Experiment

The experiment of comparing SDN-enabled MANET and OLSR is illustrated in Figure 3. The basic composition of the experiment is the same, only the way of path configuration is different. We implemented 3 nodes in simulator NS-3. Each node has a wireless interface, which is using standard IEEE 802.11g. When the scenario is set up as OLSR mode, it follows OLSR's rule. On the other hand, when it is set up as SDN enabled MANET way, an SDN controller is made, which is connected stably with each node. In this scenario, we didn't use OpenFlow as a southbound protocol. We used UDP packets when a node has to communicate with the controller.

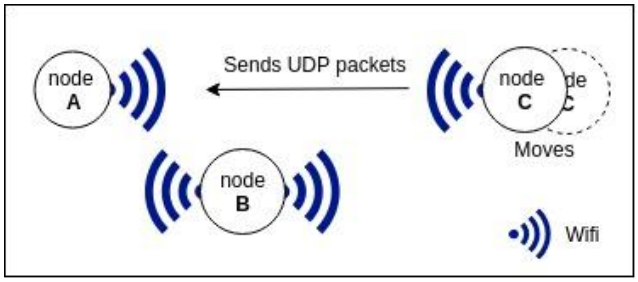

Fig. 3 Experimental Model

5.1 Experimental Scenario

1) Create Node A, B, C
2) Node C sends UDP Packets to Node A
3) Node C moves in a Node A's direction
4) Implement OLSR and SDN-enabled MANET models
5) Implement mock attacks
6) Compare the results

5.2 Experimental Results

When it comes to experiment model above, the amount of transferred bits or its speed was still better in OLSR, compared to SDN-enabled MANET's. (OLSR was 3.37Mbps during 188 seconds, SDN-enabled MANET was 1.88Mbps during 106 seconds.) We expect that's just because the experiment above do not assume complex situation.

6. Conclusion

Despite SDN and MANET is quite far concept from each other, we could see the possibility to combining to concepts. Further, we could understand what kind of security problems could be occurred in SDN based MANET, and which parameter we have to observe to estimate its availability in the future.

7. Future Work

To solve existing problems by utilizing new technology is a quite challenging approach. Because comparable data is insufficient, and lots of unexpended problems could occur. Nevertheless, to prove its availability clearly, we need to postulate various situations as possible. Hence, future work of this research is as follows.

1) Implement various SDN-enabled MANET Models in NS-3
According to the models invested above, we will perform a various experiment in NS-3. And also, we will change the value of parameters which can affect the entire network. (e.g. the number of nodes, size of packets, etc.)
2) Make various scenarios of mock attacks
We will simulate a variety of mock attacks which probably taking place in the real world. And then, compare the counteraction of pure MANET and SDN enabled MANET.
3) Improve security problems
There might be some cases that SDN enabled MANET is worse than pure MANET, even if the situation is much more complex than normal pathfinding problems. We will find and improve those kinds of cases, to make SDN enabled MANET better.

References

[1] Jang Beom-Guen, Lee Soo-Jin, "Detection and Management of Misbehaving Node in Tactical Ad-Hoc Networks", Journal of the Korea Institute of Military Science and Technology, vol.12, no.3, pp.333-343, 2009
[2] Hao Yang, Haijun Luo, Fan Ye, Songwu Lu and Lixia Zhang, "Security in Mobile Ad-Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, vol. 11, no.1, pp.38-47, 2004.
[3] K. Poularakis, G. Iosifidis, L. Tassiulas, "SDN-enabled tactical ad hoc networks: Extending programmable control to the edge", IEEE Commun. Mag., vol. 56, no. 7, pp. 132-138, Jul. 2018.
[4] Jon Spencer, Tricia Willink, "SDN in Coalition Tactical Networks", IEEE Military Communications Conference, pp.1053 – 1058, Nov. 2016
[5] Software-Defined Networking:The New Norm for Networks, https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf, Open Networking Foundation, pp.7, (visited 2019.06.21)
[6] Jeferson Nobre, Denis Rosario, Cristiano Both, Eduardo Cerqueira, Mario Gerla, "Towards Software-Defined Battlefield Networking", IEEE Commun. Mag., vol. 54, no. 10, pp. 152-157, Oct. 2016
[7] M. Jarschel, T. Zinner, T. Hossfeld, P. Tran-Gia, and W. Kellerer, "Interfaces, Attributes, and Use Cases: A Compass for SDN," IEEE Communications Magazine, vol. 52, no. 6, pp. 210–217, June 2014.
[8] Vinod K Mishra, Ayush Dusia, Adarsh Sethi, "Routing in Software-Defined Mobile Ad hoc Networks(SD-MANET)", US Army Research Laboratory Technical Report, Aug. 2018.
[9] Juliano Araujo Wickboldt, Wanderson Paim de Jesus, Pedro Heleno Isolani, Cristiano Bonato Both, "Software-Defined Networking : Management Requirements and Challenges", IEEE Commun. Mag., vol.53, no. 1, pp. 278-285, Jan. 2015