Speed Based Attacker Placement for Evaluating Location Privacy in VANET

Ikjot Saini(✉), Sherif Saad, and Arunita Jaekel

School of Computer Science, University of Windsor, Windsor, Canada
{saini11s,shsaad,arunita}@uwindsor.ca

Abstract. The deployment of connected and autonomous vehicles is expected to increase rapidly in the coming decade. For successful operation, it is critical to maintain the security and privacy of the communication messages exchanged among such vehicles. One important aspect of this is to maintain the location privacy of vehicles/users that use unencrypted basic safety messages (BSM) to exchange information with nearby vehicles. The use of temporary identifiers called pseudonyms have been proposed for protecting location privacy. A pseudonym change strategy (PCS) determines the conditions under which pseudonyms should change. The goal is to change pseudonyms in a way that prevents an attacker from linking multiple pseudonyms to the same vehicle. In this paper we explore how an intelligent attacker placement scheme can impact the success rate for linking pseudonyms. We propose a new speed-based attacker placement algorithm that can be used to evaluate different PCS. Simulation results indicate that the proposed scheme is able to increase the rate for successfully linking vehicle pseudonyms.

Keywords: VANET security · Pseudonym change
Attacker placement · Location privacy · Vehicle tracking

1 Introduction

A vehicular ad-hoc network (VANET) [1] consists of a network of vehicles, that exchange relevant information e.g. current vehicle position, vehicle state, traffic conditions, road conditions etc. to improve road safety, reduce traffic congestion and provide a variety of additional services to users. Safety applications require rapid, real-time processing of basic safety messages (BSM) sent by neighboring vehicles. In the USA, BSMs are broadcast using the IEEE 1609 WAVE protocol stack [2], built on the IEEE 802.11p [3] and are unencrypted to reduce processing time. So, anyone in the vehicles transmission range is able to receive BSMs from nearby vehicles and can use the information in successive messages to build a history of previous locations of a vehicle. Such tracking can reveal frequently visited places such as home or office location corresponding to a vehicle and compromises the privacy of the vehicle [4]. The concept of location privacy has

J. Zheng et al. (Eds.): ADHOCNETS 2018, LNICST 258, pp. 215–224, 2019.
https://doi.org/10.1007/978-3-030-05888-3_20

been defined in the literature as a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others [5]. Protecting location privacy is one of the main security challenges in VANETs [6]. To address this issue, a number of researchers have proposed the use of pseudonyms to make vehicle tracking more difficult and improve location privacy [7]. A pseudonym is a temporary identifier issued by a trusted authority. Each vehicle is issued a pool of pseudonyms and corresponding certificates that can be used, when communicating with other vehicles. The temporary certificates associated with pseudonyms also help authenticate messages sent by a vehicle.

Pseudonyms can be effective in hindering vehicle tracking only if they are changed frequently. Otherwise, an attacker may be able to link pseudonyms from the same vehicle based on its history of BSM transmissions. Furthermore, the changing of pseudonyms must be carried out in a way that makes it difficult to link 2 (or more) pseudonyms associated with the same vehicle. There has been a strong research interest in recent years, in the development of effective pseudonym change schemes (PCS) is to prevent such pseudonym linking and a number of different approaches have been proposed in the literature to address this issue [8–10]. These PCS should be evaluated not only with simplistic randomly placed attackers, but also using more sophisticated, traffic-aware attacker placement techniques.

In this paper, we propose a novel speed-based attacker placement strategy that can be used to intelligently select the most advantageous eavesdropping locations for attacking stations, based on traffic patterns and attacker capabilities. We evaluate the performance of the proposed approach and compare it with a uniformly spaced attacker placement for different road types, traffic conditions and attacker capabilities.

The remainder of the paper is organized as follows. In Sect. 2, we discuss the main types of Pseudonym Change Strategies (PCS) in VANET and some existing approaches to vehicle tracking. In Sect. 3 we describe our proposed speed-based attacker placement approach. We present our simulation results in Sect. 4 and conclude in Sect. 5 with some directions for future work.

2 Review

The location information in the vehicular networks is broadcast with a rate of 10 times per second in the safety message. The safety applications rely on this information to prevent potential collisions; however, the information broadcast is in plain text. This allows others to listen the safety messages using the dedicated equipment. The aggregated location and information gives the overall spatiotemporal resource to infer the personal information such as the personal preferences, the workplace or the medical state based on the frequent visits. The pseudonyms are used in place of the vehicle ID as these are temporary identifiers with a limited lifetime. Changing the pseudonyms reduces the ability of the passive attacker to track the vehicle. However, the knowledge of the pseudonym changing scheme and the continuous stream of safety messages with timestamped location updates allow the attacker to successfully correlate the changed pseudonym.

A number of pseudonym changing schemes have been proposed in the last few years. The fixed PCS allows the pseudonym change in a particular area, known as mix zones, or based on fixed time slot, known as periodic PCS. In [9], the concept of mix zone was first introduced and [11] implemented the cryptographic mix zone. The unobserved area is considered as the mix zone where the vehicles change the pseudonym. Also, the mix zone is the region where there are more number of vehicles and more change in the vehicles direction. Such places are intersections, parking lots or gas stations which provide enough confusion for the attacker to detect the pseudonym change. This scheme forces more frequent pseudonym changes which consumes the given set of pseudonyms in less duration. In order to prevent the exhaustion of the pseudonyms, one approach is to reuse the pseudonym for certain time period. As proposed in the most recent standards [12], 20 pseudonyms are valid for a week and the pseudonym change is periodic, i.e., after 5 min the vehicle changes the pseudonym. These schemes have an extent of predictability for the pseudonym change as these are limited to specific location or time.

The dynamic PCS change the pseudonym without predefined location or time period, making it difficult for the attacker to analyze the change of the temporary identifier. Various dynamic pseudonym changing schemes, also known as mix context schemes, are available in the literature. These schemes usually have radio silence when there is a change of pseudonym, otherwise, the change can be directly detected by the attacker. The triggers for changing pseudonyms vary from speed [13] to vehicle density [14]. The trigger-based schemes are excellent because these enable implicit trigger for a change of pseudonym. These are more effective as the attacker is not aware when vehicles are changing pseudonyms and it is not easy to correlate after an implicit trigger. Another advantage is that even if the adversary is monitoring the information, the location and time are not predetermined. Therefore, the prediction of such events is difficult, but is still possible with significant related information such as traffic analysis for the target region. The possible drawback associated with this scheme is that if there is not sufficient number of vehicles, then adversary may trace the target vehicle. Such schemes typically involve group formation for synchronous change to increase the attackers confusion. In [15], a scheme called as synchronous pseudonym change algorithm is proposed, where the status information of the vehicle and the simultaneity of the pseudonym change are considered. The concept of Random Encryption Periods for enhancing the location privacy is introduced in [16]. This PCS uses Public Key Infrastructure along with probabilistic symmetric key distribution. The symmetric key is the group based secret key which is shared among the neighboring vehicles. Weerasinghe [17] introduced the concept of a group based synchronized pseudonym changing protocol. Here the group manager decides the time to change the pseudonym and other group members are informed and after changing the pseudonym, the group is dissolved. Also, the signal strength is changed as the pseudonym is changed.

The speed based changing scheme is one of the dynamic scheme that depends on the speed threshold for the pseudonym change. SLOW was proposed for changing the pseudonym dynamically without predefined location or time. The speed threshold was proposed as 30 Km/h. According to [13], as the vehicle slows down and reaches this threshold, it changes pseudonym while maintaining the radio silence. The radio silence is not desirable for the safety applications, but with respect to the passive attacker, it prevents the continuous information broadcast that reduces the success of the linking attack. The vehicle slows down more in the city either at traffic light intersection or the stop sign causing significant rate of pseudonym change in urban areas. But it is clear that SLOW prevents the disclosure of the pseudonym change, thus, the tracking at the cost of the high number of pseudonyms. VBPC [18] is another velocity-based PCS in which the vehicles are grouped together based on the velocity within a certain transmission range and then the pseudonyms are changed based on the random time period.

3 Proposed Placement Strategy

The performance of a PCS depends on a variety of factors, such as the type of attacker (local or global), the number of attacking stations and the capabilities and communication range of the attacking station. For a local adversary with a limited number of attacking stations, the tracking success depends critically on how the attacking stations are placed. Therefore, it is important to a PCS, with a realistic and effective attacker placement. In our earlier work [19], we have shown that even a simple distance-based placement algorithm is quite effective against a periodic PCS. However, they are less successful when a dynamic PCS is used. In this section, we present a new speed-based attacker placement (SBAP) scheme that can be used for tracking vehicles using a dynamic, context-aware PCS.

3.1 Adversary Model

In our work, we have considered the local passive adversary which has limited capabilities in terms of the equipment. The communication range of the adversary is 300 m. The equipment is also named as attacking or eavesdropping station. The placement of these equipment in the simulation is according to the proposed algorithm, which allows maximum coverage with the given number of equipment. We compared the results of our placement algorithm to the uniformly distributed fixed distance placement. The communication channel is assumed to be reliable. The eavesdropping station is able to clearly listen to all the messages by the vehicles within its range. We model the attacker with limited resources to observe the maximum impact on the privacy protection. The eavesdropping stations provide the information to the central vehicle tracker that records the safety messages and correlate the location, time and pseudonym information from these messages. The vehicle tracker correlates the safety messages of a vehicle by matching pseudonyms based on the multi-target tracking algorithm [20].

3.2 Speed Based Attacker Placement

Speed based PCS relies on the speed of the vehicles. When a vehicles speed falls below a specified threshold, it changes the pseudonym. Such conditions often arise at red light intersections and stop signs. In the remainder of this paper, we refer to an intersection with a traffic light or stop sign as a Traffic/Stop Intersection (TSI). Vehicle speed can also fall below the threshold along sections of roads that experience high traffic congestion. We refer to such areas as high traffic sections (HTS). TSI and HTS are excellent candidate locations for placing attackers. However, it is infeasible wasteful to place attacking stations on all TSI or very closely spaced along a HTS. Therefore, it is necessary to identify potential attacker positions, such that fewer attackers are able to track the most number of vehicles. Successful tracking is more likely to occur when a longer stretch of the road is selected for correlation of the old and new pseudonyms of the vehicle. Therefore, we consider segments that are relatively long (at least 15 km) and have high traffic density.

Algorithm 1. Speed-based attacker placement (SBAP) algorithm

```
1: Initialize parameters: $n$=number of available equipment for tracking the vehicles,
   $r_{comm}$= Communication range of attacking station
2: Perform traffic analysis to select a set S1 of potential urban road segments for
   monitoring traffic, where $|S1| = k$ and $s_i \varepsilon S$ is the $i^{th}$ road segment.
3: Repeat steps 4 and 5 until there is no more available attacker equipment
4: For $s_i \varepsilon S1$:
   a: $loc_A$ = the location of the $1^{st}$ TSI of $s_i$
   b: Repeat steps i-iv until $loc_A \varepsilon s_i$ == False:
       i. Place attacker at $loc_A$
       ii. $d_{next}$=distance from $loc_A$ to the next TSI on $s_i$ after $loc_A$
       iii. $d_{inter} = \max\{d_{next}, 2.r_{comm}\}$
       iv. $loc_A$= $loc_A$ $+d_{inter}$
5: For all $HTS_i \varepsilon S2$:
   a: $loc_A$ = the location of the first point in $HTS_i$ that is at a distance of $2.r_{comm}$
   from previous attacker on the road.
   b: Repeat steps i-ii until $loc_A \varepsilon HTS_i$ == False:
       i. Place attacker at $loc_A$
       ii. $loc_A = loc_A + 2.r_{comm}$
```

An overview of our proposed Speed-based attacker placement is given in Algorithm 1. In step 1, we initialize relevant parameters such as the number of attacking stations (n) to place in the network, the communication range (r_{comm}) of each station. In step 2, we select certain road segments to monitor, based on long term traffic patterns. Two types of road segments are selected:

- A set $S1$ of urban roads segments where attackers will be placed based on TSI locations and
- A set $S2$ of road segments (primarily highways, but may contain some urban roads as well), where attackers will be placed based on traffic congestion.

In step 3, attackers are placed one by one on the selected road segments, based on TSI (step 4) and HTS (step 5), until all positions of interest have been covered or the maximum number of stations (n) have been used. Details of steps 4 and 5 are given below. In step 4, attacking stations are placed based on TSI locations. For each selected road segment s_i on an urban road, the first attacker is placed at the first TSI of the segment. If the distance from the current TSI to the next one is greater than $2.r_{comm}$, then an attacker is placed at the next TSI. Otherwise, next attacker is placed a location $2.r_{comm}$ from the current TSI on the road segment s_i. This placement strategy allows all the TSI along the road segment to be covered using the fewest possible attackers. In step 5, high traffic and/or congested road segments. Attackers are placed at intervals of $2.r_{comm}$ along the entire segment.

4 Results

In our simulations, we considered the area in the city of Windsor, Ontario, Canada. The simulation area contained a 15 Km stretch of Highway (H), as well as Urban(U) areas with the road network consisting of 280 edges (roads) and 120 junctions (intersections) spread in the urban area. We varied the number of available equipment from 10 to 20. This variation is used to investigate the impact of the attacker capabilities in accurately tracking vehicles for longer durations. The vehicular traffic density is varied from low to high. Higher traffic density causes traffic congestion, and this forces speed-based PCS to require more frequent pseudonym changes. To observe the effects of traffic density, we considered three levels of traffic density low (100 vehicles), moderate (200 vehicles) and high (300 vehicles). The average trip time for each vehicle was set to 2 h. We have simulated the highway and urban scenarios with separate synthetic traffics for each scenario which are generated by SUMO [21]. We setup the simulation using OMNET++ [22], SUMO, veins [23]. The trips in the urban scenario are random which means that the vehicles are traveling from different starting points to destination points.

To simulate the attackers and the privacy modules in veins [23], we have used PREXT [24], which provides a unified framework for simulating the PCS used to provide privacy in VANET. PREXT also specifies the attacking modules that listen to BSMs transmitted by the vehicles. We have placed these modules at certain observation points based on preliminary traffic analysis. In our simulations, we have compared the following four attacker placement schemes:

- the proposed SBAP scheme for urban roads (SBAP-U)
- the proposed SBAP scheme for highways (SBAP-H)
- the fixed-interval attacker placement scheme for urban roads (FIAP-U)
- the fixed-interval attacker placement scheme for highways (FIAP-H)

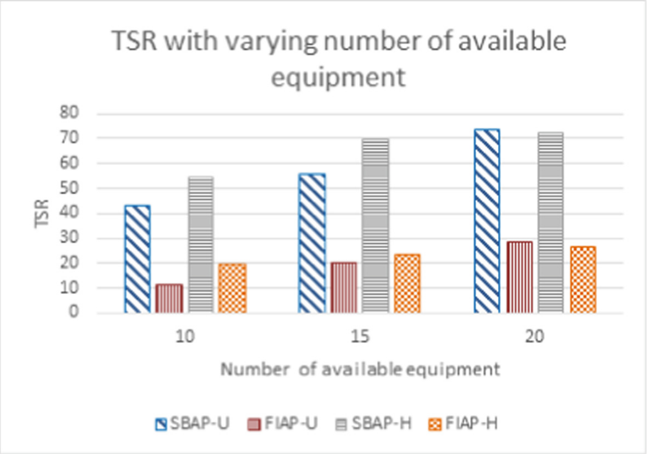

Fig. 1. Comparison of TSR values for different number of attacking stations.

The performance of these approaches is evaluated in terms of the tracking success rate (TSR), which is defined below. We map the location and time information to the respective pseudonyms and predict the vehicles next potential position. When a vehicle comes out of the silent zone, this prediction is used to identify the vehicle by matching the predicted and actual spatiotemporal information. If the matching is done correctly, we count it as a successful tracking event. When the attackers predicted position fails to correctly identify the target vehicle, it is counted as a failed tracking event. We measured the tracking success rate (TSR) as the percent-age of successful tracking events for all vehicles during their trips.

Figure 1 shows how the TSR values vary with the number of available equipment. With more number of equipment, the attacker is clearly able to track more successfully for all placement schemes, as expected. However, the TSR value of FIAP is considerably less than SBAP for both urban roads and highways. This is because for FIAP more pseudonym changes occur out of the range of the eavesdropping stations and hence remain undetected. For example, with 10 equipment in urban scenario, there are many TSIs which are not covered in the range of any attacking station. This significantly reduces the traceability as the vehicles change the pseudonyms while slowing down near TSI. Even as the number of equipment increases, the TSR remains relatively low for FIAP-U, because once a vehicle changes its pseudonym in an uncovered area, this vehicle is classified as a new vehicle by the attacker. With SBAP-U, the traceability

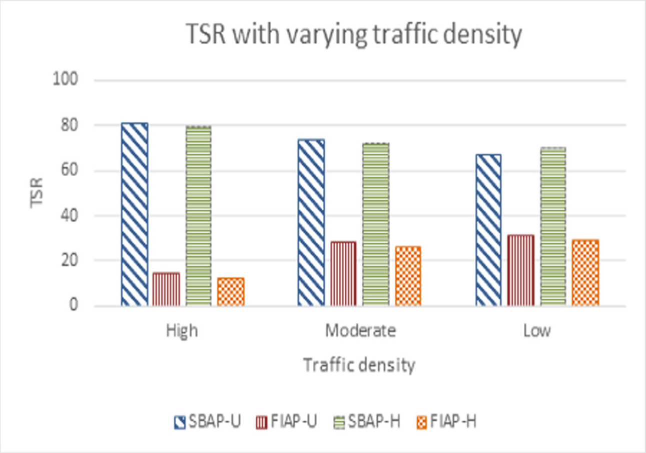

Fig. 2. Comparison of TSR values vs traffic density.

is higher as the stations are placed carefully after analyzing the traffic patterns and the busy intersections, so pseudonym changes are more likely to occur in areas being monitored by attacking equipment. The highways do not have intersections, therefore, only the traffic congestion analysis is helpful in suitable placement based on SBAP. As with urban roads, traceability increases with more number of equipment for both approaches. But, TSR for FIAP-H is consistently lower, since fewer congested areas are covered in the range of attacking stations.

The traffic density is closely related to the pseudonym change in the speed based PCS. In Fig. 2, as the number of vehicles increases, the increased traffic congestion causes the vehicles to slow down, which in turn forces the pseudonym change. If these changes occur in an area monitored by an attacker, more pseudonyms can be linked to each other. This is the case with SBAP (for both urban roads and highways) and therefore traceability increases with traffic density. For FIAP-U and FIAP-H, the rate of pseudonym change also increases with traffic density. However, many of these changes occur in unmonitored areas, so the attacker interprets the new pseudonyms as belonging to new vehicles. Therefore, the overall traceability actually decreases with traffic density. For all road types and ranges of traffic densities, the overall traceability is significantly higher (at least double) for SBAP compared to FIAP.

5 Conclusions

In this paper, we proposed a novel speed-based attacker placement (SBAP) scheme for selecting the locations of attacking stations based on analysis of long term traffic patterns. We have compared our approach to a traffic-unaware fixed interval attacker placement (FIAP) scheme and have shown that the proposed approach consistently outperforms FIAP with an average improvement of 60% in successful vehicle tracking. We conclude that attacker placement has a significant impact on the tracking capability of an attacker, given the same number and capability of attacking stations. The proposed approach can be used to evaluate different PCS and help identify potential vulnerabilities prior to deployment. The SBAP approach presented in this paper is most effective for PCS that use a velocity threshold for triggering pseudonym changes. For our future work, we plan to develop a robust attacker placement technique that be used for other context-aware PCS.

References

1. Harnstein, H., Laberteaux, L.P.: A tutorial survey on vehicular ad hoc networks. IEEE Commun. Mag. **46**(6), 164–171 (2008)
2. IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-Multichannel Operation, IEEE Std 1609.4-2010 (Revision of IEEE Std 1609.4-2006) (2011)
3. Kenney, J.: Dedicated short-range communciations (DSRC) standards in the United States. Proc. IEEE **99**(7), 1162–1182 (2011)
4. Golle, P., Partridge, K.: On the anonymity of home/work location Pairs. In: Tokuda, H., Beigl, M., Friday, A., Brush, A.J.B., Tobe, Y. (eds.) Pervasive 2009. LNCS, vol. 5538, pp. 390–397. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01516-8_26
5. Duckham, M., Kulik, L.: Location privacy and location-aware computing. In: Drummond, J., et al. (eds.) Dynamic and Mobile GIS: Investigating Change in Space and Time, pp. 34–51. CRC Press, Boca Raton (2006)
6. Emara, K.: Beacon-based vehicle tracking in vehicular ad-hoc networks, Technical report, TECHNISCHE UNIVERSITAT MUNCHEN (2013)
7. Gerlach, M.: Assessing and improving privacy in VANETs. In: Proceedings of 4th Workshop ESCAR, pp. 1–9 (2006)
8. Petit, J., Schaub, F., Feiri, M., Kargl, F.: Pseudonym schemes in vehicular networks: a survey. IEEE Commun. Surv. Tutor. **17**(1), 228–255 (2015)
9. Buttyán, L., Holczer, T., Vajda, I.: On the effectiveness of changing pseudonyms to provide location privacy in VANETs. In: Stajano, F., Meadows, C., Capkun, S., Moore, T. (eds.) ESAS 2007. LNCS, vol. 4572, pp. 129–141. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-73275-4_10
10. Li, M., Sampigethaya, K., Huang, L., Poovendran, R.: Swing and swap: user-centric approaches towards maximizing location privacy. In: Proceedings of the 5th ACM Workshop on Privacy in Electronic Society, pp. 19–28. ACM (2006)
11. Freudiger, J., Raya, M., Felegyhazi, P.P., Papadimitratos, P., Hubaux, J.P.: Mix-zones for location privacy in vehicular networks. In: ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiNITS) (2007)
12. Brecht, B., et al.: Security credential management system for V2X communications. IEEE Trans. Intell. Transp. Syst. **99**, 1–22 (2018)
13. Buttyan, L., Holczer, T., Weimerskirch, A., Whyte, W.: SLOW: a practical pseudonym changing scheme for location privacy in VANETs. In: 2009 IEEE Vehicular Networking Conference VNC, pp. 1–8 (2009)
14. Song, J.H., Wong, V.W., Leung, V.C.: Wireless location privacy protection in vehicular ad-hoc networks. Mob. Netw. Appl. **15**(1), 160171 (2010)

15. Liao, J., Li, J.: Effectively changing pseudonyms for privacy protection in vanets. In: 10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN), pp. 648–652. IEEE (2009)
16. Wasef, A., Shen, X.: Rep: location privacy for vanets using random encryption periods. Mob. Netw. Appl. **15**(1), 172–185 (2010)
17. Weerasinghe, H., Fu, H., Leng, S., Zhu, Y.: Enhancing unlinkability in vehicular ad hoc networks. In: 2011 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 161–166. IEEE (2011)
18. Ullah, I., Wahid, A., Shah, M.A., Waheed, A.: VBPC: velocity based pseudonym changing strategy to protect location privacy of vehicles in VANET. In: 2017 International Conference on Communication Technologies (ComTech), Rawalpindi, pp. 132–137 (2017)
19. Saini, I., Saad, S., Jaekel, A.: attacker placement for detecting vulnerabilities of pseudonym change strategies in VANET. In: 1st International Workshop on Dependable Wireless Communications (DEWCOM), Chicago, USA (2018)
20. Emara, K., Woerndl, W., Schlichter, J.: Beacon-based vehicle tracking in vehicular ad-hoc networks. Technical report, TECHNISCHE UNIVERSITAT MUNCHEN (2013)
21. Krajzewicz, D., Erdmann, J., Behrisch, M., Bieker, L.: Recent development and applications of SUMO-Simulation of Urban MObility. Int. J. Adv. Syst. Meas. (2012)
22. Andrs, V., Hornig, R.: An overview of the OMNeT++ simulation environment. In: Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems and Workshops, Institute for Computer Sciences, Social- Informatics and Telecommunications Engineering (2008)
23. Sommer, C., German, R., Dressler, F.: Bidirectionally coupled network and road traffic simulation for improved IVC analysis. IEEE Trans. Mob. Comput. **10**(1), 3–15 (2011)
24. Emara, K.: Poster: PREXT: privacy extension for veins VANET simulator. In: Vehicular Networking Conference VNC. IEEE (2016)