Measurement Analysis For Multi Shared Key (MSK) Based Star Topology in Various Static Environments

Mike Yuliana, Rifqi Nurfianto[1], Amang Sudarsono[2]

[1]Dept. of Electrical Engineering, Dept. of Electrical Engineering, Dept. of Electrical Engineering
[2]Politeknik Elektronika Negeri Surabaya Surabaya, Indonesia
mieke@pens.ac.id, rifqi.nurfianto111@gmail.com, amang@pens.ac.id

Abstract. Problems in the implementation of channel probing related to the correlation generated against the environment used to provide an interesting idea for conducting further analysis of channel probing in various environments in static conditions. This paper analyzed channel probing systems on ad hoc multi-user networks that form a star topology involving heterogeneous devices such as the Raspberry Pi and laptops equipped with TP-Link TL-WN722N. This method uses RSS channel parameters (received signal strength) measured by sending Ping packets with the ICMP protocol from the center to the nodes in the network. In addition, the paper also analyzes the correlation relationships between nodes in three different environmental conditions: indoor, semi-outdoor, and outdoor. The results of this paper show that different correlation relationships are depending on the environment used. Semi-outdoor environments give a correlation result of 0.4734, which makes it stronger compared to indoor and outdoor environments that are consecutive at only 0.3019 and 0.1183.

Keywords: *Ad hoc multi-user networks, star topology, channel probing systems, RSS channel parameters, heterogeneous devices, static conditions.*

1. Introduction

A multi-user ad hoc network is a type of wireless network consisting of several nodes that are interconnected without the presence of a fixed infrastructure. Star topology, in which one node acts as a center or base station communicating with other nodes, is often used in ad hoc multi-user networks to facilitate communication between nodes. Heterogeneous devices, such as the Raspberry Pi and laptops with external USB WLAN (TP-Link TL-WN722N version 1), provide diverse capabilities and play an important role in forming an efficient and flexible multi-user ad hoc network [1,2].

One of the main challenges in an ad hoc multi-user network is communication security. Generating a secure and efficient secret key becomes crucial for protecting data and privacy in the network. In this study, we will implement a channel probing system to extract secret key generation on an ad hoc multi-user network with a star topology. This method uses channel parameters, in particular, Received Signal Strength (RSS), which provides information about the signal strength received by the nodes in the network.

M. U. H. Al Rasyid and M. R. Mufid (eds.), *Proceedings of the International Conference on Applied Science and Technology on Engineering Science 2023 (iCAST-ES 2023)*, Advances in Engineering Research 230,
https://doi.org/10.2991/978-94-6463-364-1_16

Channel probing systems have been studied in the context of previous ad hoc multi-user networks [3,4]. This method allows the exploration of the characteristics of wireless channels and obtains the information necessary for the generation of secret keys. Through the delivery of Ping packets with the ICMP protocol from the center to the nodes in the network, we will collect the RSS channel parameters that reflect the signal strength received by each node. The collected RSS data will then be analyzed to identify correlation relationships between node pairs in the network.

The analysis of correlation relationships between nodes in an ad hoc multi-user network has important implications for generating secret keys and the reliability of communication [5,6]. Correlations between nodes can affect the efficiency of generating secret keys and the level of network security. In this study, we will use the Pearson correlation coefficient as a measure to measure the level of correlations between node pairs in a network. This correlation analysis will be carried out on three different environmental conditions: indoor, semi-outdoor, and outdoor.

Previous research has suggested the use of channel probing systems and correlation analysis in the context of ad hoc multi-user networks [7,8]. However, the implementation of the channel probing system on an ad hoc multi-user network with a star topology involving heterogeneous devices and the external USB WLAN TP-Link TL-WN722N version 1 as described earlier is still a field of research that has not been much explored. Therefore, the research is expected to provide new contributions to the understanding of channel probing systems in ad hoc multi-user networks with star topology.

The results of the correlation analysis of the channel probing system on an ad hoc multi-user network that forms a star topology between nodes in three different environmental conditions, namely indoor, semi-outdoor, and outdoor, using 3000 RSS data, showed differences in correlations depending on the environment used. Semi-outdoor environments have a correlation result of 0.4734, which makes it higher compared to indoor and outdoor environments, which are only 0.3019 and 0.1183, respectively. This suggests that semi-outdoor environments have stronger correlation relationships between nodes in the network.

2. Related Works

This review of the library aims to present the theoretical framework and related research on the implementation of channel probing systems on ad hoc multi-user networks with star topology involving heterogeneous devices and external USB WLAN TP-Link TL-WN722N version 1. Through this review of the library, the basic concepts of multi-user ad hoc networks, channel probing systems, the use of channel parameters like RSS (received signal strength) in the generation of secret keys, and the analysis of correlation relationships between nodes in ad hoc multi-user networks will be discussed.

An ad hoc multi-user network is a wireless network consisting of several nodes connected dynamically without a fixed infrastructure. Star topology, in which one node acts as a center or base station communicating with other nodes, is often used in ad hoc multi-user networks [9]. Heterogeneous devices such as the Raspberry Pi and laptops with external USB WLAN (TP-Link TL-WN722N version 1) provide flexibility and versatility in forming an efficient multi-user ad hoc network [10].

In this context, channel probing systems become an interesting method for extracting secret key generation in an ad hoc multi-user network with a star topology. Channel probing utilizes channel parameters, in particular received signal strength (RSS), to obtain information about the signal strength received by the nodes in the network. This method has previously been studied in the context of an ad hoc multi-user network [1]. By collecting RSS data through the delivery of Ping packets with the ICMP protocol from the center to the nodes in the network, the channel probing system can generate a secure and efficient secret key [6].

In addition, the analysis of the correlation relationship between nodes in an ad hoc multi-user network also plays an important role in generating the secret key and ensuring the reliability of communication [8]. Correlation relationships between node pairs in a network can affect the level of security and effectiveness of secret key generation. In this study, the Pearson correlation coefficient will be used as a measure to measure the level of correlations between node pairs in a network [3]. This correlation analysis will be carried out on three different environmental conditions, namely indoor, semi-outdoor, and outdoor, to understand the environmental influence on correlational relationships in the network.

Several previous studies have proposed and analyzed the use of channel probing systems and correlation analysis in the context of multi-user ad hoc networks [4,7]. However, the implementation of channel probing systems on ad hoc multi-user networks with star topologies involving heterogeneous devices and external USB WLAN (TP-Link TL-WN722N version 1) as described above is still a limited field of research. Therefore, this research will make an important contribution to the understanding and development of channel probing systems on an ad hoc multi-user network with this specific configuration.

3. Multi Shared Key Based Star Topology

A. **Device Description and Network Configuration**

In this section, a description is made of the devices used in this study, such as the Raspberry Pi, laptop, and the TP-Link TL-WN722N external USB WLAN. Additionally, an ad hoc multi-user network configuration with a star topology consisting of a central or base station (1 Raspberry Pi), 4 nodes (3 Raspberry Pi and 1 laptop), as well as 1 adapter, is described. (1 buah Raspberry Pi). Each device is equipped with an external USB WLAN to enable wireless connectivity between nodes.

Generating a multi-shared key is an important step in ensuring the security of communication between several wireless devices. Previously, the Received Signal Strength (RSS) key extraction scheme only applied to pairing devices that communicate with each other. In this study, we focused on implementing channel probing systems for a group of heterogeneous wireless devices by collecting RSS data collaboratively. However, there are some challenges in using RSS measurement for generating multi-shared keys. First, RSS values between devices cannot be delivered securely, complicating the process of key agreements between devices. Second, if the device in the group moves, the RSS-based method becomes inapplicable because the device may be outside the reach of communication. To address this, we used a metric called the Difference of Signal Strength (DOSS) to facilitate key extraction [11].

MSK-Based Star Topology Extraction. We also consider scenarios where all devices in the group are within reach of communication with each other, such as in the case of a group of students studying together in a cafe who want to communicate safely. We use a one-device star topology as a virtual center node that facilitates multi-shared key extraction by sharing DOSS values with other devices in the group. In this section, we will explain the multi-shared key extraction protocol through the star topology we have used.

Design of Protocol. There are four steps to be followed in the protocol through the star topology. We assume that there are n nodes in the group, and each member of the group is represented by j, with j = c,1,2,...,n-1.

The first step is the random selection of one of the group members as a virtual center node (for example, node c), which will be used to extract a secret key based on a radio channel between the central node and another randomly selected node, such as node 1. Figure 1 shows an illustration of the topology with the central node and other multi-members. At each time slot t, starting from t = 1 to T, the group repeats steps 2–3.

The second step involves each member of the group j, with j = 1,··,n-1, to obtain the measurement of the channel $Y_{c,j}^{j}$(t) by exchanging the probe package with the central node and quantifying the observation with the accuracy level Δ. The observation is then spotted to the nearest multiplication of the whole number of Δ to obtain a quantified observation, $Y_{c,j}^{\Delta,j}$(t). At the same time, the central node c receives the reinforcement of the channel, $Y_{j,c}^{c}$(t), from all the node members j.

The third step involves calculating the DOSS value by the center node c using the equation as shown in (1):

$$\delta_j(t) = Y_{j,c}^{c}(\mathrm{t}) - Y_{1,c}^{c}(\mathrm{t}), \tag{1}$$

for j, j = 2,···, n-1. Next, the quantified DOSS value, δ_j^{Δ}(t), is transmitted by the central node.

The final step is to be able to initiate a one-way public discussion at a central node, where the initial key bits are extracted through information reconciliation. After the information is reconciled, all nodes will have the same initial key, but some information is also disclosed to the attacker. Furthermore, the nodes undergo privacy amplification to produce a secret key that is independent of all observations, including those heard during public discussions. Topology and broadcast illustrations are presented in Figure 1.

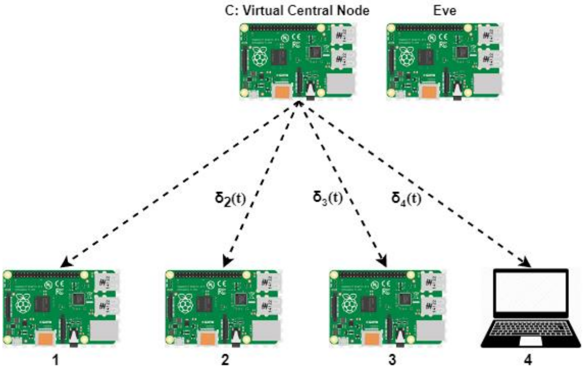

Fig. 1. Illustration of star topology for multi-shared key extraction protocol

The attack model. We take into account the existence of a passive attacker called the Sniper, who follows legitimate mobile devices involved in multi-shared key extraction. The transmitter performs observations of channel strengthening independently of other legitimate mobile device channel enhancement observations. The speaker can listen to all the public discussions that take place during the key generation and obtain the secret key extraction algorithm along with the parameters used for key generation [12]. It is assumed that the scanner is at least λ/2 away from the legitimate device. At half-wave lengths, wireless channel reinforcements experience random correlations in multipath fading environments, so observations on the transducer and the legitimate node become independent. This ensures that the insider cannot obtain information about legitimate channel reinforcement solely based on observations on the channel itself [13]. However, by collecting channel information broadcast during the public discussion phase from several wireless devices, hackers may be able to obtain part or all of the multi-shared keys as the number of users increases. To address this, the next phase of privacy amplification must be carried out by the legitimate user.

B. RSS data collection through channel probing

In this section, we describe the steps of collecting data on RSS (received signal strength) through the channel probing method. The measurement process is carried out by sending Ping packets using the ICMP protocol from the center to all the nodes in the network. Each device uses Wireshark software that is in monitor mode to record and collect RSS data. Measurement is carried out in a static condition to ensure consistency of the measurement results.

We implemented this channel probing system scheme on the 2,417 GHz channel in the area of building D4 Politecnik Elektronika Negeri Surabaya. In this experiment, we used the TP-Link TL-WN722N external WiFi module that works at a 2.4 GHz frequency with a standard IEEE 802.11b/g/n wireless adapter. On devices configured as central, as well as on devices configured as valid node clients and unauthorized node customers (Eve), they are all equipped with a virtual monitor interface to capture received packets. The Wireshark application, as a virtual monitor interface, runs to record all received packages. The experiment is carried out by sending 4000 ICMP

PINGs from Central to a valid node-node, where every package of ping requests received by the node will be followed by a ping response package. Packets captured by Wireshark are filtered using an IP address to obtain a list of desired packets.

In this experiment, all the devices involved operated with the Raspbian OS operating system. We perform RSS measurements with configuration settings performed using different wireless devices (heterogenous) and types of movement in silent conditions(static). Since the frequency of the carrier used is 2,417 GHz, we ensure that Eve is more than λ/2 = 6.25 cm [14] by placing Eve 50 to 100 cm away from Central so that no useful information is obtained by Eve.

There are three scenarios used in testing the implementation of the channel probing system in this multi-user environment. Scenarios with indoor conditions, scenarios with conditions in partially open areas, and scenarios in open areas. (outdoor). Figure 2 shows a scenario with conditions in room E-107 (Lab. Telephony) as an indoor environment. Central, as the initiator, is on the table to the left of the first row of tables, while valid nodes are on the tables to the right and left of the third-row and fourth-row tables. While Eve was at the table to the right of the first row of the table or the table next to the central table. The distance between central node 2 and node 3 is between 5 and 7 meters, while the distance between nodes 4 and 5 is between 9 and 11 meters. The distance between Eve and Central is 1 meter.

Figure 3 shows a measurement scenario with conditions in the front area or terrace between the E-107 room and the lecturer room as a semi-outdoor environment, where the layout configuration and distance of each of the devices involved in this scenario are as shown in the image. Figure 4 shows a measurement scenario with conditions in the basketball field area as an outdoor environment, where a clearer illustration related to the layout configuration and the distance of each of the devices involved in this scenario can be seen in the picture. It should be remembered that all devices involved at the time of measurement are in a silent position (static).

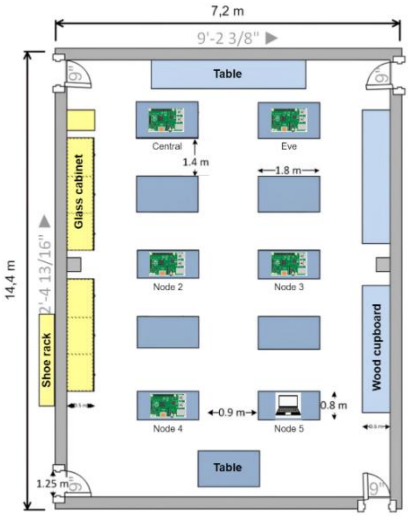

Fig. 2. Measurement scenarios in indoor conditions

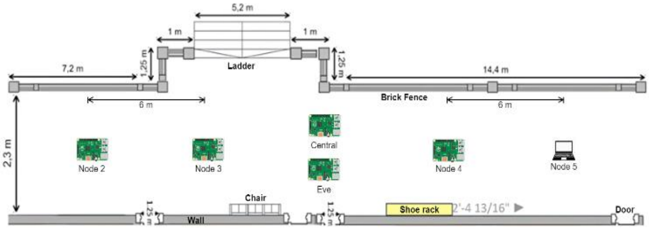

Fig. 3. Measurement scenarios in semi-outdoor conditions

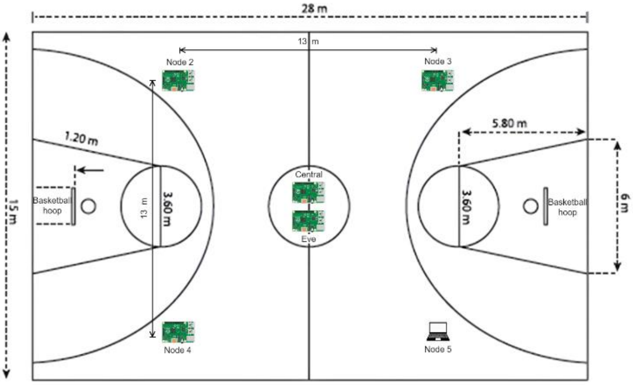

Fig. 4. Measurement scenarios in outdoor conditions

C. Measurement scenarios in outdoor conditions

This section explains the processing and analysis of the data that has been collected. The RSS data collected from each node is processed to obtain relevant information. Data processing processes include outlier removal, data normalization, and grouping based on environmental conditions. Next, statistical analysis is performed to identify correlation relationships between nodes in an ad hoc multi-user network.

D. Measurement of correlation between nodes

This section explains the method for measuring the correlation between nodes in a network. In this study, the Pearson correlation coefficient was used as a measure of correlation. RSS data that has been processed and grouped according to environmental conditions is used to calculate the correlation coefficient between each pair of nodes in the network. This correlation measurement provides insight into the reliability of communication between nodes and the environmental influence on the correlational relationships formed. The correlation values range between +1 and -1. A value of +1 indicates a perfect positive linear relationship, while a value of -1 shows a perfect negative linear relationship. If the value of the correlation coefficient is 0, then there is no linear relationship between the two variables in question [15]. To find the value of the correlation coefficient ($r_{A,B}$) between the two measurement data sets, RSS results, for example, in Alice and Bob, can be found using the equation shown in (2):

$$\mathrm{r}y^{A}y^{B} = \frac{N\sum\ (Y^{A}Y^{B})-(\sum\ Y^{A})(\sum\ Y^{B})}{\sqrt{\left[N\sum\ (Y^{A})^{2}-\left(\sum\ Y^{A}\right)^{2}\right]\left[N\sum\ (Y^{B})^{2}-\left(\sum\ Y^{B}\right)^{2}\right]}} \quad (2)$$

Where $\mathrm{r}y^{A}y^{B}$ is the value of the Pearson correlation coefficient, N is the amount of RSS measurement data analyzed, y^{A} is the RSS channel parameter measured by Alice, y^{B} is the RSS channel parameter measured by Bob.

Through this research, it is expected to gain an in-depth understanding of the implementation of channel probing systems on ad hoc multi-user networks with star topology. In addition, the correlation analysis between nodes will provide important information to improve the reliability of communication in ad hoc multi-user networks relevant to different environmental conditions.

4. Results And Analysis

E. **RSS data in indoor environments**

This section explains the results of the measurement and analysis of RSS data collected in indoor environments. After performing data processing, information is obtained about the signal strength received by each node in an ad hoc multi-user network. These results provide an overview of the level of reliability of communication between nodes in indoor environments. In addition, correlation analysis between nodes in this environment is carried out to understand the correlational relationships formed.

The amount of net RSS data obtained by each valid node at the time of measurement with indoor conditions within room E-107 (Lab. Telephony) is 3750 data points, with RSS values ranging from -40 to -89 dBm. While the amount of RSS data obtained by an Eve is only 2200 data points, with RSS values ranging from -44 to -72 dBm. From the amount of RSS data obtained, it may indicate that the evader (Eve) does not always get the RSS value of the number of ping packets sent by the central device.

Then, from the previous RSS value data, we need to convert it into DOSS form first before calculating the correlation coefficient value. Furthermore, the result of the formed DOSS correlation is displayed graphically, as shown in Figure 5 for conditions obtained from valid nodes with the highest data spread at DOSS 1 in the range of 1 to 10 dBm and Figure 6 for conditions derived from unauthorized nodes (Eve) with the greatest data spread at DOSS 2 in the interval of -9 to 0 dBm.

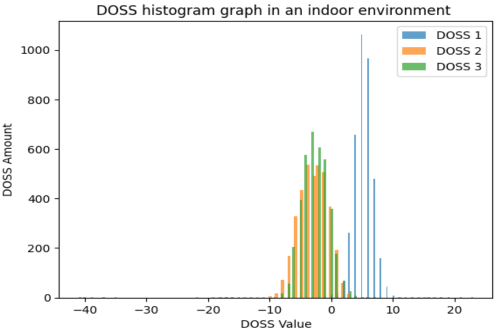

Fig. 5. DOSS histogram in the indoor environment

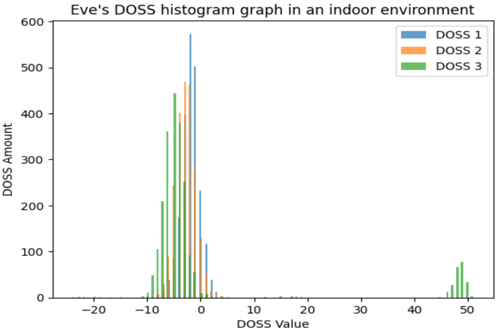

Fig. 6. DOSS Eve histogram in the indoor environment

F. **RSS data in semi-outdoor environments**

In this section, the results of the measurement and analysis of RSS data performed in a semi-outdoor environment are described. The RSS data collected from each node is analyzed to obtain information about the strength of the signal and the correlation relationships between the nodes in this environment. These results provide insight into the performance of communication in semi-outdoor conditions and the factors that influence it.

The amount of net RSS data obtained by each valid node at the time of measurement with semi-outdoor conditions in the front area or terrace between the E-107 room and the lecturer room is 3650 data points, with RSS values ranging from -28 to -74 dBm. While the amount of RSS data obtained by an Eve is only 2900, with RSS values ranging from -27 to -71 dBm.

The result of the formed DOSS correlation is displayed graphically, as shown in Figure 7 for conditions obtained from valid nodes with the highest data spread found in DOSS 2 at the range of 11 to 20 dBm, and Figure 8 for conditions derived from unauthorized nodes (Eve) with the greatest data distribution found in DOSS 2.

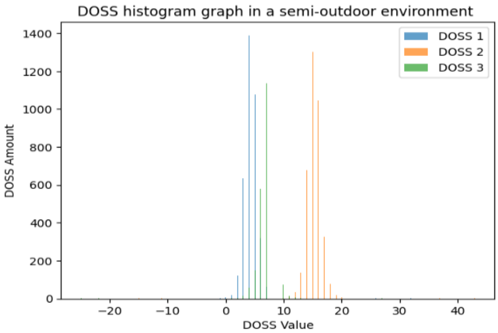

Fig. 7. DOSS histogram in a semi-outdoor environment

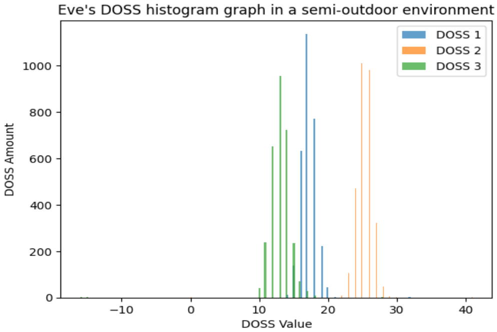

Fig. 8. DOSS Eve histogram in a semi-outdoor environment

G. RSS data in outdoor environments

This section explains the results of the measurement and analysis of RSS data in outdoor environments. The RSS data collected from each node is analyzed to gain an understanding of signal strength and correlation relationships between nodes in outdoor environmental conditions. These results provide important information about the effectiveness of communication in ad hoc multi-user networks in outdoor environments that may have different challenges, such as interference and changing weather conditions.

The amount of net RSS data obtained by each valid node at the time of measurement with outdoor conditions in the basketball field area is 3600 data points, with RSS values ranging from -41 to -88 dBm. While the amount of RSS data obtained by an Eve is only 1350, with RSS values ranging from -41 to -77 dBm.

The result of the formed DOSS correlation is displayed graphically, as shown in Figure 9 for the conditions obtained from valid nodes with the highest data spread at DOSS 1 in the range of 1 to 10 dBm and Figure 10 for conditions obtained from unauthorized nodes (Eve) with the largest data spreads at Doss 1 and DOSS 2 at the interval of 1 up to 10 dBm.

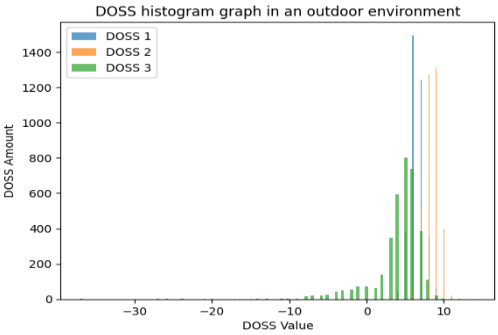

Fig. 9. DOSS histogram in an outdoor environment

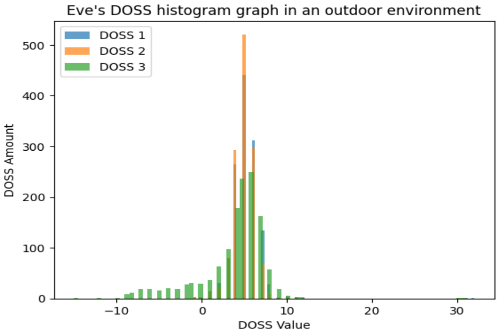

Fig. 10. DOSS Eve histogram in an outdoor environment

H. Correlation analysis between nodes

In this section, a correlation analysis is carried out between nodes in an ad hoc multi-user network. Based on the RSS data collected from each environment, the Pearson correlation coefficient is calculated for each pair of nodes in the network. The results of this analysis provide insight into the strength of correlation relationships between nodes in various environmental conditions. In addition, this analysis also helps in understanding the influence of heterogeneous devices and network topology on the correlation relationships formed.

Based on the information presented in Table 1, the correlation coefficient between valid nodes is 0.3019 in indoor conditions, 0.4734 in semi-outdoor conditions, and 0.1183 in outdoor conditions. This suggests that the correlation coefficient values in semi-outdoor environmental conditions tend to be higher with strong correlations between nodes than in indoor and outdoor environmental conditions. This is because in indoor conditions there are many challenges, such as interference and disruption of physical and property barriers between the PC, wardrobe, and table. In outdoor conditions, there is a challenge because the distance between the nodes or the gap between the node and the central is so far away that the correlation formed is small.

Based on Table 1, it is also seen that the correlation coefficient formed between DOSS Eve and DOSS Central in various conditions appears to be quite low. This is because at a distance of more than half the wavelength, the wireless channel reinforcement experiences random correlations in the multipath fading environment, so that the observation on the interceptor (Eve) against the valid nodes becomes independent, and as a result, the results of the RSS values captured by Eve are not similar to the RSS values captured by the central device. Therefore, it will be very difficult for the sinker (Eve) to obtain information about the amplification of the same RSS channel with valid nodes only based on observations on the sicker channel itself.

TABLE I. COMPARISON OF CORRELATIONS IN DIFFERENT ENVIRONMENTAL CONDITIONS

Scenario	**Coefficient of Correlation**	
	DOSS between legitimate nodes	**DOSS Central - DOSS Eve**
Indoor	0.3019	0.0319
Semi-outdoor	0.4734	0.0538
Outdoor	0.1183	0.1510

Through these results and analyses, it is expected to gain a comprehensive understanding of communication performance and correlation relationships between nodes in ad hoc multi-user networks. This information can be used to improve the reliability of communication in a variety of environments and help in designing an efficient and reliable multi-user ad hoc network.

5. CONCLUSION

Implementation of channel probing systems in ad hoc multi-user networks with star topology using heterogeneous devices, such as Raspberry Pi and laptops with external USB WLAN TP-Link TL-WN722N, has been successfully carried out and has proven to have the potential to improve the reliability of communication between nodes. RSS data collection through ICMP Ping protocol package delivery and correlation analysis between nodes is carried out in three environmental conditions, namely indoor, semi-outdoor, and outdoor. Each environmental condition has a significant influence on the correlation relationship and reliability of communication, with semi-outdoor environments tending to provide a stronger correlation result of 0.4734 compared to indoor and outdoor environments, which were consecutive at 0.3019 and 0.1183, respectively.

Future research is expected to test this channel probing system in more complex scenarios with a larger number of nodes and environmental variations, as well as with more sophisticated external WLAN devices. This will help broaden the understanding of the reliability of communication in a diverse and dynamic multi-user ad hoc network.

References

1 A. R. Pratama, D. K. Rini, and H. B. Santoso, "Performance Analysis of Channel Probing Techniques in Wireless Ad Hoc Networks," Proc. 2019 *IEEE International Conference on Advanced Computer Science and Information Systems* (ICACSIS), pp. 267-272, 2019.

2 X. Li, M. Jiang, and J. Li, "Correlation Analysis in Multi-hop Wireless Ad Hoc Networks," Proc. 2018 *IEEE International Conference on Wireless Communications, Signal Processing and Networking* (WiSPNET), pp. 86-91, 2018.

3 P. Gupta and P. K. Srivastava, "Analyzing Correlation and Impact of Node Density on Ad Hoc Networks," Proc. 2017 *International Conference on Advances in Computing, Communication and Automation* (ICACCA), pp. 1-5, 2017.

4 M. A. Kousa, S. N. Othman, and A. Z. Hasan, "Channel Probing in Ad Hoc Networks: A Survey," *IEEE Access*, vol. 8, pp. 218350-218368, 2020.

5 L. Chen, Y. Sun, and J. Ma, "Secret Key Generation Scheme Based on Correlation of Channel State Information in Ad Hoc Networks," Proc. 2020 *IEEE/CIC International Conference on Communications in China* (ICCC), pp. 230-235, 2020.

6 W. Cui, T. Zhang, and S. Ji, "Correlation Analysis of Channel State Information for Secret Key Generation in Ad Hoc Networks," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2389-2402, 2018.

7 H. A. Boubakr and S. Kallel, "Channel State Information Based Secret Key Generation Scheme for Wireless Ad Hoc Networks," Proc. 2017 *International Conference on High Performance Compilation, Computing and Communications* (HP3C), pp. 153-158, 2017.

8 X. Zheng, X. Huang, and D. Wang, "Efficient Secret Key Generation in Wireless Ad Hoc Networks via Channel State Information," Proc. 2019 *IEEE/CIC International Conference on Communications in China* (ICCC), pp. 439-444, 2019.

9 J. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 6-28, 2004.

10 L. S. Shieh, C. C. Huang, and Y. C. Tseng, "An Adaptive Data Forwarding Mechanism for Heterogeneous Wireless Sensor Networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 1, pp. 96-109, 2014.

11 H. Liu, Jie Yang, Yan Wang, Yingying Chen and C.Emre Koksal, “Group Secret Key Generation via Received Signal Strength : Protocols, Achievable Rates, and Implementation”, *IEEE Transactions on Mobile Computing*. 2013.

12 M. Yuliana, Wirawan dan Suwadi, “Skema Secret Key Generation (SKG) Untuk Keamanan Pada Sistem Komunikasi Di Lingkungan Wireless,”2018,[Online]. Available:https://repository.its.ac.id/70392 2018

13 A. Goldsmith, *Wireless Communications*. New York, NY, USA: Cambridge University Press, 2005.

14 M. Yuliana, Wirawan and Suwadi, “Performance Evaluation of the Key Extraction Schemes in Wireless Indoor Environment,” *Conf.IEEE 2017 International Conference on Signals and Systems*, ICSIgSys, Bali, Mei. 2016.

15 R. C. Tripathi, A. Kumar, and M. R. Senapati, "Performance parameter in the form of Pearson correlation coefficient for measuring linear dependence between users' RSS measurements," in 2017 *International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)*, Chennai, India, 2017, pp. 360-364. doi: 10.1109/ICEECCOT.2017.8284575 . 2017