A Physical Layer Security-based Routing Protocol in Mobile Ad-hoc Wireless Networks

Kyusung Shim*, Tri Nhu Do*†, and Beongku An‡
*Dept. of Electronics and Computer Engineering in Graduate School, Hongik University, Republic of Korea
‡Dept. of Computer and Information Communications Engineering, Hongik University, Republic of Korea
Emails: *shimkyusung@outlook.kr, †dotrinhu@gmail.com, ‡beongku@hongik.ac.kr

***Abstract*—Physical layer security has been considered as a sustainable technique that is competitive with existing cryptographic approaches to combat security attacks in the next generation wireless networks. In this paper, we study the vulnerability of mobile ad-hoc wireless networks in which there is an eavesdropper monitoring for the data transmissions in the networks. To this end, we propose a Physical Layer Security-based Routing protocol, called PLSR, which uses ad-hoc on-demand distance vector as the underlying technology. The main features and contributions of the proposed PLSR are as follows. First, PLSR considers a cross-layer approach that uses the information of both physical layer and network layer together to support QoS transmission (i.e., secure transmission) efficiently. When a routing route is established, both the physical layer information, PLS information using distance between neighbors an eavesdroppers, and the network layer information, i.e., the number of hops, are considered together as the parameters for route establishment. Second, PLSR establishes the routing routes that can avoid the eavesdroppers to support secure transmission. The performance evaluation of the proposed PLSR using OPNET shows that PLSR can efficiently support the security capability of routing and multi-hop transmission in mobile ad-hoc wireless networks.**

***Keywords*—routing, physical layer security, cross-layer, MANETs**

I. Introduction

Mobile ad-hoc networks (MANETs) is the ad-hoc networks consisting of mobile nodes. Different from the infrastructure-based networks, MANETs do not have a fixed manager node, i.e., access point (AP) or base station (BS), while all nodes can work as router. Thus, MANETs are characterized by direct communication or multi-hop communication without a manager node. MANETs have the advantage that the networks configuration is easier than the infrastructure-based networks. The famous routing protocol in MANETs is ad-hoc on-demand distance vector (AODV) routing protocol [1]. AODV consists of two processes that are reverse path setup and forward path setup to make the routing route. During the reverse path setup, a source and intermediate nodes broadcast a route request (RREQ) packet to find a destination. When receiving the RREQ, the destination unicasts a route reply (RREP) packet using the shortest path. When the source node receives the RREP, the route establishment process is completed. Then, the source node forwards the data packets via the established route.

Recently, the security issue is an attractive research topic in MANETs. These networks are vulnerable to an attack of malicious users because the networks do not have the manger nodes [2], [3]. The authors of [4] proposed the secure and efficient MANET routing protocol called SAODV to prevent black hole attack. This routing protocol generates a random number to confirm the legitimate destination. The authors of [5] proposed secure routing protocol (SRP) using underlying dynamic source routing protocol (DSR) in MANETs. This routing protocol established the trust route between a source and a destination. The wormhole attack prevention(WAP) routing protocol is proposed in MANETs [6]. This routing protocol used the special list called neighbor list to detect the wormhole attack. This protocol detected the wormhole attack and updated this route information to prevent the attack of the malicious node.

On the other hand, in sniffing attacks, the eavesdroppers only overhear and collect information in the networks. It seems to be hard to combat against sniffing attacks in wireless mobile networks. Specifically, the authors of [7] demonstrated the sniffing attack through the fake hotspot. In [8], the authors studied the security threats in machine-to-machine (M2M) networks. The authors proposed the countermeasures on the sniffing that encrypts the data packet by using a hardware security module (HSM) to prevent the data packet from the sniffing attacker that did not decrypt the encrypted data because sniffing attacker did not have HSM.

The traditional TCP/IP model has advantages in terms of maintenance and development. However, this model does not efficiently support the quality of service (QoS) in the networks. Researchers have studied the cross-layer approach to improve the network performance and satisfy the requirement of future networks. The authors of [9] surveyed facing problems in stack-based architectures and the requirements of the future networks. The encryption methods such as SSL, SSH, WEP can support the secure transmissions in the TCP/IP model. However, These encryption methods increase the processing power, leading to the added energy consumption and latency. Therefore, the research on secure routing applying cross-layer approach is needed.

Recently, physical layer security (PLS: PHY-security) technique has been considered as a promissing solution to protect the information through the wireless nature of medium by exploiting the physical characteristics of wireless channels to securely transmit information between legitimate users [10]–[12]. The authors of [13] studied the PHY-security and

challenges in industrial wireless sensor networks. The authors demonstrated that the increased number of antenna of sink increased the security performance. In [14], the authors studied PHY-security for the future networks. The authors summarized the PHY-security issue that is the trusted relay and untrusted relay, and the challenges such as massive multiple-input multiple-output (MIMO), mm-wave on the future networks. The authors of [15] studied PHY-security in the tree topology composed of the multi-hop wireless networks with multi-eavesdropper.

Different from the mentioned related works, in this paper, we propose a physical layer security-based routing protocol to prevent the sniffing attacks and support secure transmission by utilizing the emerging PHY-security concepts. The main features and contributions of this paper are summarized as follows:

- We propose a physical layer security-based routing protocol, called PLSR, that can support the secure multi-hop transmission using cross-layer approach. PLSR uses the physical layer information (i.e., PLS information) and network layer information (i.e., number of hops) together to establish the secure routing route.
- PLSR establishes a secure route by using the PHY-security concept. More specially, a mobile node that is required to communicate with other one first broadcasts the RREQ packet to establish a fresh route to a targeted node. During the RREP procedure, the destination and intermediate nodes broadcast the RREP to estimate the secure ability (i.e., PLS ability) which is measured based on the difference in distance between that from a transmitter to a receiver and that from a transmitter to a eavesdropper.
- The simulation results are also provided to demonstrate the performance of the secure transmission of the PLSR that successfully avoids the coverage of eavesdropping while PDR is maintained similar to AODV.

The rest of the paper is arranged as follows. Section II introduces the basic concepts and architecture of PLSR and describes in detail the route establishment process. Section III presents the performance metrics compared PLSR to AODV. Finally, the conclusions are given in Section IV.

II. The Physical Layer Security-based Routing Protocol (PLSR)

A. The Basic Concepts and Architecture of PLSR

Let us present the motivation of PLSR, i.e., the underlying idea of PHY-security is identified as a promising method that achieves secure communications by smartly exploiting the imperfections of the wireless channel [16]. In PHY-security, the secrecy capacity C_S can be given by

$$C_S = C_{\text{main}} - C_{\text{eve}}, \tag{1}$$

where C_{main} means the channel capacity of the main link between Alice and Bob. Similar to the main channel definition, the term C_{eve} represents the channel capacity of eavesdropper link between Alice and Eve. The each channel capacity can be represented by using signal-to-noise ratio (SNR). The secrecy capacity can be expressed as

$$C_S = \log_2\left(1 + \mathtt{SNR}_{\text{main}}\right) - \log_2\left(1 + \mathtt{SNR}_{\text{eve}}\right), \tag{2}$$

where $\mathtt{SNR}_{\text{main}}$ and $\mathtt{SNR}_{\text{eve}}$ are the main channel and eavesdropper channel, respectively. Considering the free-space path loss model [17], the received power can be given by

$$P_{\text{r}} = P_{\text{t}} G_{\text{t}} G_{\text{r}} \frac{\lambda^2}{\left(4\pi d\right)^2}, \tag{3}$$

where the G_{t} and G_{r} are the transmit and receive antenna gains and λ represents the wavelength and d means separation of transmitter antenna and receiver antenna, respectively. Plugging (3) into (2), C_S can be rewritten as

$$\begin{aligned} C_S &= \log_2\left(1 + \frac{P_{\text{r,main}}}{\text{N}_0}\right) - \log_2\left(1 + \frac{P_{\text{r,eve}}}{\text{N}_0}\right) \\ &= \log_2\left(1 + P_{\text{t}} G_{\text{t}} G_{\text{r,main}} \frac{\lambda^2}{\left(4\pi d_{\text{main}}\right)^2 \text{N}_0}\right) \\ &\quad - \log_2\left(1 + P_{\text{t}} G_{\text{t}} G_{\text{r,eve}} \frac{\lambda^2}{\left(4\pi d_{\text{eve}}\right)^2 \text{N}_0}\right), \end{aligned} \tag{4}$$

where $P_{\text{r,main}}$ and $P_{\text{r,eve}}$ are the received power at the legitimate node and eavesdropper, respectively. Similar to received powers, the term $G_{\text{r,main}}$ and $G_{\text{r,eve}}$ are the legitimate node and eavesdropper antenna gains, respectively. N_0 means the additive white Gaussian noise (AWGN) power. In order to guarantee the secure of the communication, it is required that C_S is greater than 0 for successful secure transmission which can be expressed as

$$\log_2\left(1 + \frac{P_{\text{t}} G_{\text{t}} G_{\text{r,main}} \lambda^2}{\left(4\pi d_{\text{main}}\right)^2 \text{N}_0}\right) > \log_2\left(1 + \frac{P_{\text{t}} G_{\text{t}} G_{\text{r,eve}} \lambda^2}{\left(4\pi d_{\text{eve}}\right)^2 \text{N}_0}\right), \tag{5}$$

which is equivalent to

$$\frac{P_{\text{t}} G_{\text{t}} G_{\text{r,main}} \lambda^2}{\left(4\pi d_{\text{main}}\right)^2 \text{N}_0} > \frac{P_{\text{t}} G_{\text{t}} G_{\text{r,eve}} \lambda^2}{\left(4\pi d_{\text{eve}}\right)^2 \text{N}_0}. \tag{6}$$

In this paper, we assume that the legitimate nodes and eavesdropper have the same performance ability that is the $G_{\text{r,eve}}$ equals to $G_{\text{r,main}}$. Thus, after some algebraic manipulations, (7) can be obtained as

$$\frac{1}{d_{\text{main}}} > \frac{1}{d_{\text{eve}}}. \tag{7}$$

The relationship in (7) means that the further the distance from the transmitter, the smaller the channel capacity and the smaller signals can be received. Thus, when an eavesdropper locates further than next node, the received signal can not be completely decoded at the eavesdropper.

Fig. 1 describes the basic concepts and architecture of the proposed protocol. In the given networks, S is a source node that transmits data packets when events occur, while D presents a destination node that receives the data from the source node via routing route and E denotes the eavesdropper

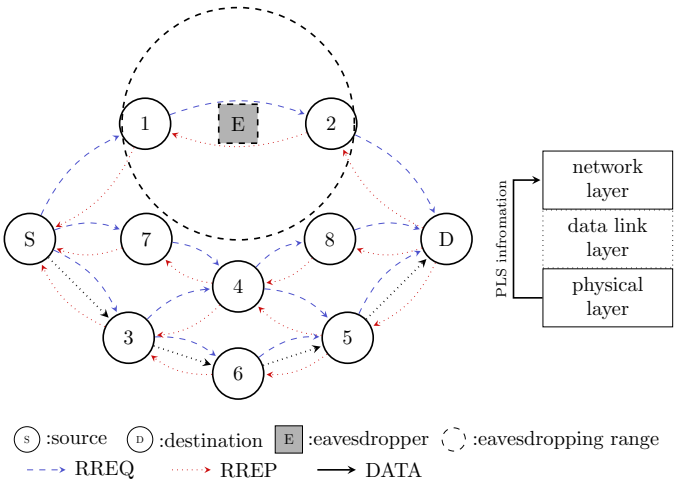

Fig. 1. The basic concepts and architecture of PLSR

that monitors the multi-hop transmission from S to D. PLSR is proposed to aim to avoid the overhearing range of the eavesdropper and to support secure transmission by using cross-layer strategy with physical layer and network layer. As we can see in Fig. 1, the shortest path is S $\rightarrow$ 1 $\rightarrow$ 2 $\rightarrow$ D. However, PLSR does not establish the shortest route because the route is within the overhearing range of the eavesdropper, E. Instead of the shortest path, PLSR adopts (7) to establish the route, specifically, the distance difference from the transmitter to between next node and malicious node. As the result, the established path is S $\rightarrow$ 3 $\rightarrow$ 6 $\rightarrow$ 5 $\rightarrow$ D. The proposed PLSR can establish a routing route that can avoid the eavesdropping range and support secure transmission using cross-layer strategy with physical layer and network layer.

B. The Routing Algorithms used in PLSR Protocol

In this subsection, we describe in detail the proposed PLSR protocol. When an event occurs, the source node broadcasts the RREQ to find the destination. The RREQ packet contains the following fields :

$$\langle \texttt{SourceID}, \texttt{DestinationID}, \texttt{SrcSeq}, \texttt{DestSeq}, \texttt{BroadcastID}, \texttt{hopcount} \rangle$$

where the SrcSeq is called source sequence and DestSeq denotes destination sequence, which are the identified number to confirm control message, respectively. BroadcastID means the number of generating RREQ on the same session at the source. hopcount presents the number of intermediate node toward the destination. When the neighbor nodes of the source receive the RREQ packet, the intermediate nodes confirm whether the RREQ packet is enough to fresh through Algorithm 1 or not. The received node confirms whether SrcSeq is greater than the value in its table or not. The nodes update the routing table while the intermediate nodes rebroadcast the RREQ with the increment hopcount, and the destination transmits the RREP to select the further node from eavesdropper toward the source with the increment DestSeq.

Algorithm 1 The RREQ transmission procedure of PLSR

Condition: When the node receives the RREQ packets from neighbor nodes.

if $\texttt{SrcSeq}_{\text{RREQ}} > \texttt{SrcSeq}_{\text{table}}$ **then**
  Update route table
  if $\texttt{nodeID} = \texttt{destination}$ **then**
    Transmit RREP
  else
    $\texttt{hopcount}_{\text{RREQ}} \leftarrow \texttt{hopcount}_{\text{RREQ}} + 1$
    Send RREQ
  end if
else if $\texttt{SrcSeq}_{\text{RREQ}} = \texttt{SrcSeq}_{\text{table}}$ **then**
  if $(\texttt{BroadcastID}_{\texttt{RREQ}} > \text{BroadcastID}_{\text{table}})$ OR $((\texttt{BroadcastID}_{\texttt{RREQ}} = \text{BroadcastID}_{\text{table}})$ AND $(\texttt{hopcount}_{\text{RREQ}} + 1 < \texttt{hopcount}_{\text{table}}))$ **then**
    Update route table
    if $\texttt{nodeID} = \texttt{destination}$ **then**
      Transmit RREP
    else
      $\texttt{hopcount}_{\text{RREQ}} \leftarrow \texttt{hopcount}_{\text{RREQ}} + 1$
      Send RREQ
    end if
  end if
else
  Drop RREQ
end if

Different from AODV, PLSR broadcasts the RREP to select the furthest node from an eavesdropper. The RREP packet contains the following fields:

$$\langle \texttt{DestinationID}, \texttt{SourceID}, \texttt{DestSeq}, \texttt{hopcount}, \texttt{LocationInformation}(\texttt{x}, \texttt{y}) \rangle$$

where $\texttt{LocationInformation}(\texttt{x}, \texttt{y})$ is the position information of transmitter. The receiving node calculates the difference distance from the node to its previous node and from the node to its eavesdropper to select the furthest distance different. Hence, the next node will be selected as

$$\texttt{nodeID}_{\text{next}} = \arg \max_{\text{N}_i \neq \text{N}_j} \left\{ d_{\text{N}_i\text{E}} - d_{\text{N}_i\text{N}_j} \right\}, \qquad (8)$$

where N_i is the RREP receiving node and N_j is the RREP transmitting node. $d_{\text{N}_i\text{E}}$ is the distance from receiving node to the eavesdropper and $d_{\text{N}_i\text{N}_j}$ is the distance from the receiving node to the transmitting node. As receiving the RREP, the nodes check whether the RREP is duplicated or not according to Algorithm 2 where d_{cost} denotes the maximum difference distance between from the receiving node to eavesdropper and from the receiving node to transmitting node. According to Algorithm 2, the intermediate node repeats this process until the RREP arrived at the source node. The source node transmits the data packets to the destination node through the established route. Fig. 2 illustrates the RREP packet format of PLSR at OPNET.

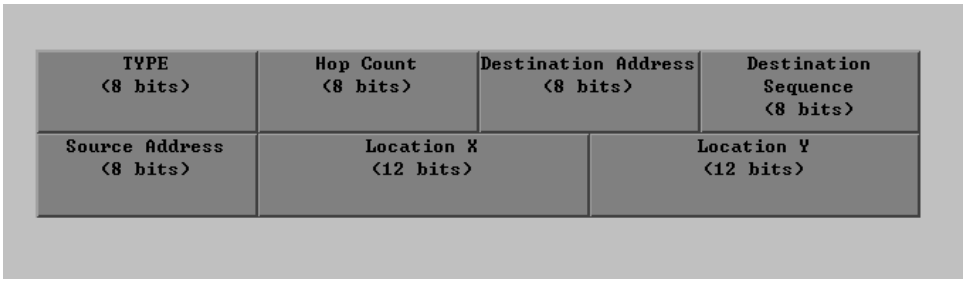

Fig. 2. The RREP packet format of PLSR

Algorithm 2 The RREP transmission procedure of PLSR

Condition: When the node receives the RREP packets from neighbor nodes.

if $(\texttt{DestSeq}_{\text{RREP}} > \texttt{DestSeq}_{\text{table}})$ OR $((\texttt{DestSeq}_{\text{RREP}} = \texttt{DestSeq}_{\text{table}})$ **then**
  if $d_{\text{N}_i\text{E}} > d_{\text{N}_i\text{N}_j}$ **then**
    if $d_{\text{N}_i\text{E}} - d_{\text{N}_i\text{N}_j} > d_{\text{cost}}$ **then**
      Update route table
      if $\texttt{nodeID} = \texttt{source}$ **then**
        Transmit DATA
      else
        $\texttt{hopcount}_{\text{RREP}} \leftarrow \texttt{hopcount}_{\text{RREP}} + 1$
        Send RREP
      end if
    end if
  end if
else
  Drop RREP
end if

III. Performance Evaluation

In this section, we present the performance evaluation of the proposed PLSR protocol with comparisons to that of the conventional AODV protocol using OPNET. The simulation environments and parameters used in this paper are listed in the following Table I.

TABLE I
Simulation Parameters

Parameters	Value
Network size	$1,000 \times 1,000$ (m^2)
Network topology	homogeneous Poisson point process (PPP)
Number of node	50
Number of eavesdropper	1
Antenna type	omni-directional antenna
Communication range	250 (m)
Path loss model	free-space path loss (Friis path loss)
Simulation Time	1,200 (s)
Data interarrival time	exponential(1)
Mobility model	random way point
Pause time	10 (s)
Node speed	5, 10, 15, 20 (m/s)

We consider a network whose size is 1 km by 1 km, 50 legitimate nodes are located in this network by homogeneous Poisson point process, and one misbehavior is located at the middle of the network to collect data. Each node is assumed to be aware of its position with a reliable position location system. Additionally, each node is equipped with an omnidirectional antenna with the transmission range of 250 m. We assume that the wireless environment is free-space path loss model in MANETs. The antenna gains equals to 1 because each node is equipped with omnidirectional antenna [18]. The mobility model of legitimate nodes is random way point [19].

The network performances are evaluated in terms of the following metrics:

- *Packet delivery ratio* (PDR): the ratio of the number of the received data packet at a destination node over the number of the transmitted packet at a source node.
- *Delay*: the average latency time for the route establishment between a source and a destination.
- *Control overhead*: the average number of control signal message per node to establish a routing route between a source node and a destination node.
- *Average distance*: the average distance from a data transmitter to an eavesdropper.

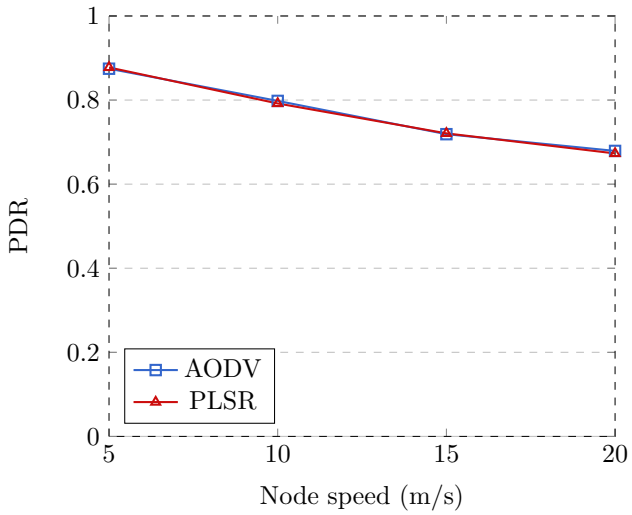

Fig. 3. Packet delivery ratio of PLSR and AODV as a function of node speed

Fig. 3 presents the PDR as a function of node speed. As can be seen in Fig. 3, the PDR decreases as the node speed increases because the higher node speed, the weaker the link connectivity between transmitter and receiver. The PDR of PLSR is similar to that of AODV, which means that the transmission performance of PLSR is similar to that of AODV.

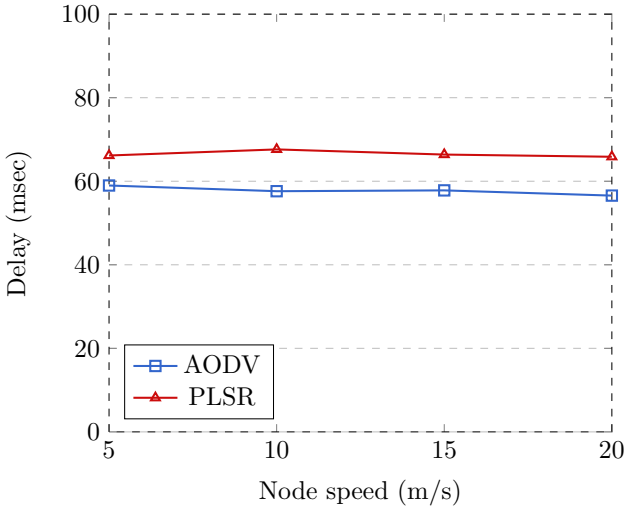

Fig. 4. Delay of PLSR and AODV as a function of node speed

In Fig. 4, we plot the delay as a function of node speed. As can be seen in Fig. 4, the delay is nearly constant as node speed increases, which means that the node speed does not effect on delay. However, the delay of PLSR is a little bit greater than AODV. The reason is that PLSR establishes the route through more nodes to avoid misbehavior.

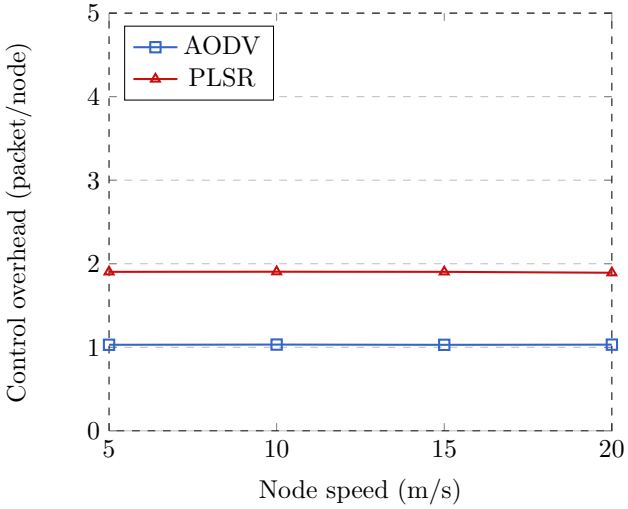

Fig. 5. Control overhead of PLSR and AODV as a function of node speed

As we can see in Fig. 5, the control overhead of PLSR is a little bit greater than that of AODV. The reason is that PLSR need to broadcast the RREP toward the source to support secure transmission while AODV just uses unicast for RREP transmission toward the source.

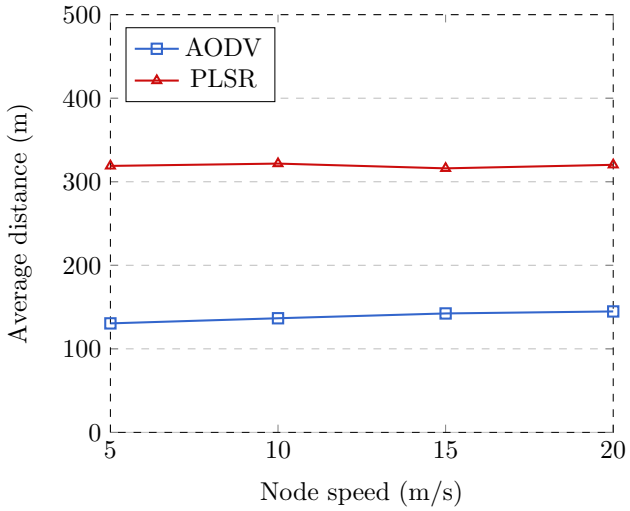

Fig. 6. Average distance of PLSR and AODV as a function of node speed

Fig. 6 presents the average distance as a function of node speed. As can be seen in Fig. 6, the average distance of PLSR is over the 300 m, which means that most of nodes in a secure route are out-of-range of the eavesdropping range, 250 m. On the contrary, using AODV protocol, most of nodes in the established route are possible in the observation range of the eavesdropper since the average distance is around 100 m, which means that the AODV protocol may be vulnerable to the eavesdropper's attack.

From Fig. 3 to Fig. 6, we can conclude that PLSR efficiently provides the secure transmission to avoid the range of eavesdropping while PLSR consumes a little bit more delay and control overhead than AODV.

IV. Conclusions

In this paper, we propose a physical layer security-based routing protocol, called PLSR. This protocol applies to cross-layer approach by combing physical layer and network layer to support secure transmission in MANETs successfully. Distance is performed in the physical layer to measure the channel capacity for PLS information while the information of number of hop is used for establishment of routing route in the network layer with cross-layer concepts. The performance evaluation shows that the proposed PLSR can efficiently support the secure transmission with fine PDR while control overhead and delay to establish secure routing route are spent a little more than that of AODV.

Acknowledgments

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (Grant No. 2016R1D1A1B03934898) and by the Leading Human Resource Training Program of Regional Neo industry Through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and future planning (Grant No. 2016H1D5A1910577).

REFERENCES

[1] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications*, Feb. 1999, pp. 90–100.

[2] A. Sgora, D. D. Vergados, and P. Chatzimisios, "A survey on security and privacy issues in wireless mesh networks," *Security and Communication Networks*, vol. 9, no. 13, pp. 1877–1889, Sep. 2013.

[3] M. Hollick, C. Nita-Rotaru, P. Papadimitratos, A. Perrig, and S. Schmid, "Toward a taxonomy and attacker model for secure routing protocols," *ACM SIGCOMM Computer Communication Review*, vol. 47, no. 1, pp. 43–48, Jan. 2017.

[4] S. Lu, L. Li, K. Y. Lam, and L. Jia, "SAODV: A manet routing protocol that can withstand black hole attack," in *Proceedings of 2009 International Conference on Computational Intelligence and Security*, vol. 2, Dec. 2009, pp. 421–425.

[5] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, Jan. 2002, pp. 193–204.

[6] S. Choi, D. Y. Kim, D. H. Lee, and J. I. Jung, "WAP: Wormhole attack prevention algorithm in mobile ad hoc networks," in *Proceedings of 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, Jun. 2008, pp. 343–348.

[7] A. H. Khoula, N. Shah, and A. N. S. Shankarappa, "Smartphone's hotspot security issues and challenges," in *Proceedings of 11th International Conference for Internet Technology and Secured Transactions 2016*, Dec. 2016, pp. 113–118.

[8] G. Tuna, D. G. Kogias, V. C. Gungor, C. Gezer, E. Takn, and E. Ayday, "A survey on information security threats and solutions for Machine to Machine (M2M) communications," *Journal of Parallel and Distributed Computing*, vol. 109, pp. 142–154, Nov. 2017.

[9] G. Carneiro, J. Ruela, and M. Ricardo, "Cross-layer design in 4G wireless terminals," *IEEE Wireless Communications*, vol. 11, no. 2, pp. 7–13, Apr. 2004.

[10] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. of the National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

[11] B. A. Kyusung Shim, Tri Nhu Do, "Performance analysis of physical layer security of opportunistic scheduling in multiuser multirelay cooperative networks," *Sensors*, vol. 17, no. 2, p. 377, 2017.

[12] K. Shim, N. T. Do, B. An, and S. Y. Nam, "Outage performance of physical layer security for multi-hop underlay cognitive radio networks with imperfect channel state information," in *2016 International Conference on Electronics, Information, and Communications (ICEIC)*, Jan. 2016, pp. 1–4.

[13] J. Zhu, Y. Zou, and B. Zheng, "Physical-layer security and reliability challenges for industrial wireless sensor networks," *IEEE Access*, vol. 5, pp. 5313–5320, Apr. 2017.

[14] H. C. Yiliang Liu and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys and Tutorials*, vol. 19, no. 1, pp. 347–376, FIRST QUARTER 2017.

[15] W. Saad, X. Zhou, B. Maham, T. Basar, and H. V. Poor, "Tree formation with physical layer security considerations in wireless multihop networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 11, pp. 3980–3991, Nov. 2012.

[16] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[17] H. T. Friis, "A note on a simple transmission formula," *Proceedings of the IRE*, vol. 34, no. 5, pp. 254–256, May 1946.

[18] W. Stallings, *Wireless Communications & Networks (2nd Edition)*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 2004.

[19] D. B. Johnson and D. A. Maltz, *Dynamic Source Routing in Ad Hoc Wireless Networks*. Boston, MA: Springer US, 1996.

Kyusung Shim received the B.S degree in computer and information communications engineering from Hongik University, South Korea, in 2012, and the M.S. degree in information system from Hongik University, in 2017. He is currently pursuing the Ph.D. degree in electronics and computer engineering with Hongik University. He is also a Teaching Associate in electronics and computer engineering with Hongik University. His main research topics are wireless communications and cooperative relaying transmissions.

Tri Nhu Do was born in Da Nang, Vietnam. He received the B.S. degree in electronics and telecommunications engineering from the Posts and Telecommunications Institute of Technology, Vietnam, in 2012, and the M.S. degree in electronics and computer engineering from Hongik University, Sejong Campus, South Korea, in 2015. He is currently pursuing the Ph.D. degree in electronics and computer engineering with Hongik University. He is also a Teaching Associate in electronics and computer engineering with Hongik University. His main research topics are wireless communications and cooperative relaying transmissions.

Beongku An received the M.S. degree in electrical engineering from the New York University (Polytechnic), NY, USA, in 1996 and Ph.D. degreefrom New Jersey Institute of Technology (NJIT), NJ, USA, in 2002, BS degree in electronic engineering from Kyungpook National university, Korea, in 1988, respectively. After graduation, he joined the Faculty of the Department of Computer and Information Communications Engineering, Hongik University in Korea, where he is currently a Professor. From 1989 to 1993, he was a senior researcher in RIST, Pohang, Korea. He also was lecturer and RA in NJIT from 1997 to 2002. He was a president of IEIE Computer Society (The Institute of Electronics and Information Engineers, Computer Society) in 2012. From 2013, he also works as a General Chair in the International Conference, ICGHIT (International Conference on Green and Human Information Technology). His current research interests include mobile wireless networks and communications such as ad-hoc networks, sensor networks, wireless internet, cognitive radio networks, ubiquitous networks, cellular networks, and IoT. In particular, he is interested in cooperative routing, multicast routing, energy harvesting, physical layer security, visible light communication (VLC), crosslayer technology, mobile cloud computing. Professor An was listed in Marquis Whos Who in Science and Engineering, and Marquis Whos Who in the World, respectively.