Anonymous Secure Routing Protocol for Wireless Metropolitan Networks

Ren-Junn Hwang[1], and Yu-Kai Hsiao [2]
junhwang@ms35.hinet.net [1], Shiaukae@gmail.com [2]
Department of Computer Science and Information Engineering Tamkang University Taipei,Taiwan

Abstract—*This paper proposes efficient concepts of anonymous and secure routing protocol considering symmetric and asymmetric communication models for Wireless Metropolitan Networks. A wireless metropolitan network is a group of wireless access points and several kinds of wireless devices (or nodes) in which individual nodes cooperate by forwarding packets for each other to allow nodes to communicate beyond the symmetric or asymmetric model. Asymmetric communication is a special feature of Wireless Metropolitan Network because of the different wireless transmission ranges of wireless devices. With asymmetric communication model, message exchange can be more efficient in metropolitan scale network. Providing security and privacy in Wireless Metropolitan Networks has been an important issue over the last few years. This paper proposes concepts of routing protocol beyond symmetric and asymmetric model, which guarantees security and anonymity of the established route in a hostile environment, such as Wireless Metropolitan Networks. The routes generated by the proposed concept are shorter than those in prior works. The wireless clients out of access point wireless transmission range may anonymously discover a secure route to connect to the access point for Internet access via the protocol based on the proposed concepts. The proposed concepts enhance wireless metropolitan network coverage in assuring security and anonymity.*

Keywords: Asymmetric communication, Wireless metropolitan networks, Secures routing, Anonymous routing

1 Introduction

Wireless Metropolitan network (WMNs) integrates several kinds of networks such as ad hoc networks and wireless infrastructure networks in metropolitan area. This kind of network is formed by access point and wireless clients. Wireless client can be any kind of wireless device. Access points function as a gateway/bridge in negotiating different kinds of networks. It allows wireless devices with different communication protocols to communicate each other and provide a larger wireless coverage area than traditional wireless networks.

Wireless metropolitan networks (WMNs) combine several kinds of wireless devices. Each device may provide different communication and computation capability. WMNs provide different communication styles. In the WMN scenario in Figure 1, User *S* has a larger transmission range than *A* and *B*. Both *A* and *B* can receive messages from *S* directly, but only *A* can reply to *S* directly. *B* can reply to *S* via *A* indirectly. This paper names the adjacent users of WMNs in communication using the symmetric model if they communicate each other directly such as Users (*S*, *A*) and Users (*A*, *B*) in Figure 1. The user names its partner as the regular-neighbor if they can communicate in the symmetric model. This paper names the adjacent users of WMNs in communication using the asymmetric model if the user can communicate with its partner directly but the partner can only communicate with it via another user indirectly, such as Users (*S*, *B*) in Figure 1. The user names its partner as semi-neighbor if it communicates with its partner directly but the partner can only communicate with it via another user indirectly. The partner names the user as its rev-semi-neighbor. For example, User *B* is User *S*'s semi-neighbor and User *S* is User *B*'s rev-semi-neighbor in Figure 1. The WMN includes both symmetric and asymmetric models for each adjacent user, while the wireless ad hoc network only provides a symmetric model. The WMNs will enhance or provide more functionality based on communication in the asymmetric model.

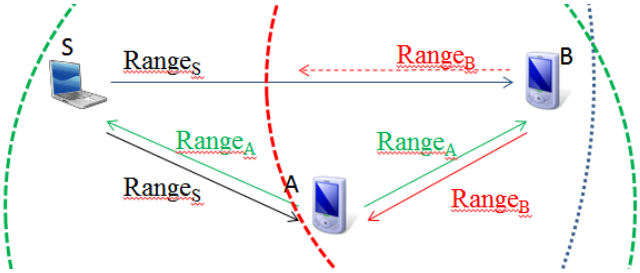

Figure 1. Scenario of communication in symmetric and asymmetric models.

In general, the transmission range of the access point is generally larger or equal to that of the wireless client. Access point not only serve wireless client directly as the traditional wireless network, but also serves wireless clients that can only communicate with it via some other wireless clients indirectly with asymmetric communication model. The wireless client in WMNs functions as both the client and router to made networks work well. The coverage of WMNs will be enhanced by this feature. By this case, the traditional routing protocols are not suitable for WMNs to generate the routing path between access point and wireless client. Some researches [2][5] [12][13][16][18] provide routing protocols with well consideration for this kind of networks. However, these protocols focus only on the efficiency and effectiveness. In wireless metropolitan networks, all data transmissions are usually via wireless transmission. It made eavesdropping, replace and modified message are easy occurred. Wireless metropolitan networks are also vulnerable to several kinds of attacks such as the Sybil attack [10], Rushing Attack [8], and etc... .

The routing protocol will fail to establish a corrected rout because several kinds of attacks corrupt the transmitting data. Secure routing protocols will straighten out these threats. Secure routing protocols have to guarantee data integrity and confidentiality and ensure the data will reach the correct destination. Several secure routing protocols [1][3][6][7][11][14] for wireless ad hoc and sensor networks provide mechanisms that resist attacks and guarantee that the destination will receive the correct transmitted data. These secure routing protocols consider only the symmetric communication model. The secure routing protocol of WMNs should consider both symmetric and asymmetric communication models to enhance the efficiency of WMNs.

Although the routing security protocol provides some security functionalities, the adversary will collect network traffic to analyze user behavior. The adversary may invade the user's privacy and hurt the user's safety. Some researches [1][4][14][16] proposed anonymous routing protocols to preserve privacy. Some studies have also considered anonymous data transmission to prevent the adversary from tracing messages to discover the sender. These anonymous routing protocols also only consider the symmetric communication model.

The communication of wireless client should consider both symmetric and asymmetric models to enhance the efficiency of WMNs. However, previous secure [7][7][9][11][15][17] or anonymous [1][4][14][16] routing protocols cannot work the communication in asymmetric model. Some attacks such as the Sybil attack and Rushing attack occur easily in asymmetric communication model. This paper proposes an anonymous secure routing protocol for WMNs. The protocol based on proposed concepts will generate an efficient anonymous and secure routing path for the access point and its wireless clients based on symmetric and asymmetric models. This paper first provides the *neighbor discovery concept* for each user to discover its regular-neighbor, semi-neighbor and rev-semi-neighbor in Section 2. Each user in WMNs will use the proposed *neighbor discovery concept* to authenticate its neighbors and establish shared keys with them. The authentication and shared keys are essential to provide reliable data dissemination and ensure data confidentiality and integrity. Section 3 proposes a concept of anonymous and secure routing protocol. The protocol based on the proposed concepts considers when users cannot connect to access point directly, they can perform this protocol to establish an anonymous and secure route to the access point and obtain internet service securely. Access point can serve more users and increase the coverage of WMNs base on the proposed concept. Some simulation results and discussions are included in Section 4. Section 5 makes presents conclusions.

There are two main roles in the WMN: access point and wireless client. Access point integrates different communication protocols and provides internet service for the wireless client in WMNs. Wireless client is the user of WMNs. Access point and wireless client hold public/private key and a broadcast key that use to protect messages when broadcasting to their neighbors. Table 1 defines the notations of the proposed concepts.

TABLE I. NOTATIONS

Notations	Means
PK_i/SK_i	The public/private key of role i.
K^b_i	The broadcast key of role *i*
K_{ij}	The shared secret key of role *i* and role *j*
N_i	A random nonce of role *i*
$Sign_i(M)$	A unrecovered signature of message *M* that signed by role *i*
p	A large prime number.
g	A generator of Z_p^*
$MAC(K,M)$	Message Authentication Code of message *M* using key *K*
$E(K,M)$	Encrypt message *M* using key *K*
NL_i	The neighbor list of role i.
NCL_i	The neighbor candidate list of role i.
$H()$	A hash function.
$Sign_i(*)$	A unrecovered signature of message before the signature
$MAC(K,*)$	Message Authentication Code of message before it using key *K*
$H(*)$	A hash for message before it.

2 Neighbor discovery concept

This section proposes the neighbor discovery concept in wireless metropolitan networks with asymmetric

communication consideration. Each user maintains two kinds of neighbors; one is regular-neighbor and the other is semi-neighbor. The user named a regular-neighbor of the request user, which receives the neighbor discovery message from the request user directly and can authenticate with the request user directly. The user named semi-neighbor of the request user, which receives neighbor discovery message directly but can only authenticate the request user via request user's other regular-neighbors or semi-neighbors indirectly. The user will be named a rev-semi-neighbor of its semi-neighbor. For example, in Figure 1, if *S* is the request user, *A* authenticates with *S* directly but *B* can only authenticate *S* via *A*. *A* is a regular-neighbor of *S*, *B* is a semi-neighbor of *S* and *S* is a rev-semi-neighbor of *B*.

In the proposed neighbor discovery concept, the user first performs the *regular-neighbor discovery phase* and then performs the *semi-neighbor discovery phase* to discover its regular-neighbors and semi-neighbors. User cannot communicate with its rev-semi-neighbor directly. User should perform the *data forwarding to rev-semi-neighbor method* (as Subsection 2.3) to communicate with its rev-semi-neighbors while it communicates with its regular-neighbors and semi-neighbors directly.

2.1 Regular-neighbor discovery phase

Each user and access point in the wireless metropolitan network performs the *regular-neighbor discovery phase* to discover their regular-neighbors. In the scenario of Figure 1, User *S* first generates Neighbor discovery message T^S_1.

$$T^S_1=\{ID_S||N_S||g^{r_S} \bmod p||\ Sign_S(*)\}.$$

Users such as User *A* and User *B* verify Message T^S_1 and generate the reply message. User *A* records *S* in its Neighbor Candidate List NCL_A User *A* chooses a random number r_A and computes $g^{r_A} \bmod p$. User *A* computes the shared secret key $K_{SA} = (g^{r_S})^{r_A} \bmod p$. Then User A replies message T^A_2 to User *S*.

$$T^A_2=\{ID_S||ID_A||g^{rA} \bmod p||\ Sign_A(H(ID_S||\ ID_A||K_{AS}))\}$$

User *B* replies a message T^B_2 as T^A_2, but User *S* cannot receives T^B_2 because *S* is out of User *B*'s transmission range. User *S* computes $K_{AS} = (g^{r_A})^{r_S} \bmod p$ and verifies T^A_2. User *S* records User *A* as regular-neighbor in Neighbor List NL_S. User S replies message T^S_3 to User A.

$$T^S_3= \{ID_S||E(K_{AS}, K^b_S||H(K^b_S))||\ Sign_S(ID_S||\ ID_A||N_S)\}$$

User *A* records $Sign_S(ID_S||ID_A||N_S)$ and removes *S* from NCL_A after verifies and decrypts T^S_3. After above procedures, each user will recognize its regular-neighbor after the *regular-neighbor discovery phase*. It also gets a shared secret key with each regular-neighbor and each regular-neighbor's broadcast key.

2.2 Semi-neighbor discovery phase

If User's neighbor candidate list is not empty after *regular-neighbor discovery phase*, it performs the *semi-neighbor discovery phase* to discover the semi-neighbors from the neighbor candidate list. In the scenario of Figure 1, *A* recognizes *B* and *S* as its regular-neighbors and gets their broadcast keys $\{K^b_B, K^b_S\}$and shared secret keys $\{K_{AB}, K_{AS}\}$ after *A* performs the *regular-neighbor discovery phase*. *B* recognizes *A* as its regular-neighbor and get *A*'s broadcast key K^b_A and shared secret key K_{AB}, but *S* is still keep in *B*'s neighbor candidate list NCL_B after *S* and *B* perform the *regular-neighbor discovery phase*. To authenticate *S*, *B* broadcasts the message T^B_4.

$$T^B_4=\{ID_B||NCL_B||\ MAC(K^b_B, ID_B||NCL_B)\}$$

User adjuncts to User B such as User A verifies T^B_4 and generates the reply message T^A_5 to *B*. User *A* computes the common neighbor list $NL_{B,A,}$.

$$NL_{B,A} = NCL_B \cap NL_A.$$

If $NL_{B,A}$ is not empty, User *A* sets the $SignList_{B,A}$= $\{Sign_j(ID_j||ID_A||N_j)|\ \forall j \in NL_{B,A}\ \}$ and replies message T^A_5 to *B*.

$$T^A_5=\{ID_A||NL_{B,A}||SignList_{B,A}||\ MAC(K_{AB},\ NL_{B,A}||\ SignList_{B,A}\ )\}$$

User *B* replies message T^B_6 to User *S* via User *A* after verifies message T^A_5.

$$T^B_6=\{ID_S||ID_B||g^{r_B} \bmod p||Sign_B(\mathrm{H}(ID_B||ID_S||K_{BS}))\}$$

User *S* computes shared secret key K_{BS} via Diffie-Hellman key exchange and record User *B* as semi-neighbor in NL_S after verifies message T^B_6. User S replies message T^S_7 to User B.

$$T^S_7=\{ID_S||E(K_{BS},K^b_S||H(K^b_S))\ ||Sign_S(ID_S||\ ID_B||N_S)\}$$

User *B* obtains the broadcast key K^b_S and records $Sign_S(ID_S||ID_B||N_S)$. User *B* records User *S* as rev-semi-neighbor and User *A* as the corresponding common neighbor in NL_B. After User *B* authenticates User *S*, User B re-computes $NL_{B,j} = NCL_j \cap NL_B$ for each User *j* in NL_B. If $NL_{B,j}$ is not empty, User *B* notifies User *j* that they have common neighbors via send the message form as message T^A_5.

2.3 Data forwarding to rev-semi-neighbor method

This subsection proposes *Data forwarding to rev-semi-neighbor method*. When User *i* tries to forward message *m* to its rev-semi-neighbor User *j*. User *i* forward $\{ID_k||E(K_{ik}, ID_j||m||H(*))\}$ to their recognized neighbor User *k* which is maintained in NL_i at the *semi-neighbor discovery phase*. User *k* keeps forward the message decrypts and $\{ID_j||m||H(*)\}$ to User *j* after User *k* decrypt and verified the message. If User *j* is User *k's* rev-semi neighbors, User *k* forward message as User *i*'s form. Otherwise, User *k* sends $\{ID_j||m||H(*)\}$ to User *j* directly.

3 A concept of anonymous secure routing protocol

If user in WMNs would like to access Internet, it should first connect to the access point. User that is a regular-neighbor of the access point can communicate with the access point directly to access the Internet. The user that cannot connect to the access point directly must establish a route to the access point to access Internet. It is important to guarantee the data can reach the correct destination and the received data is confident and correct. To protect the user privacy is also an important issue in the connection with the access point. The user's communication behavior cannot be learned by an adversary. This section provides a concept of anonymous and secure routing protocol to establish a route that achieves authentication, confidentiality, integrity and anonymity. The user that cannot connect with the access point directly performs the protocol based on the proposed concept to establish an anonymous and secure route to the access point after performing neighbor discovery concept as Section 2. The proposed concept includes *anonymous route request phase* and *anonymous route reply phase*. The user will establish an anonymous and secure route to access point after performing the protocol based the proposed concept detailed in Subsections 3.1 and 3.2.

3.1 Anonymous route request phase

User *S* performs the *anonymous route request phase* to discover an anonymous and secure route to the target destination, Access point *D*. Source *S* first generate the $ARREQ_s$.

$$ARREQ_s = \{E(K^b_S, TPK||\ E(PK_D, ID_D||TSK||PL_S)||\ Route\_Sec_S\ ||\mathrm{H}(*))\}.$$

$ARREQ_s$ is formed by three parts. The first part is the *TPK*, the temporal public key which is generated by User *S* only for this session. User *S* also generates the corresponding temporal private key *TSK*. The second part is $E(PK_D, ID_D||TSK||PL_S)$. User *S* uses destination's public key to encrypts destination's real identity ID_D, the temporal private key *TSK* and the PL_S which is the length of random padding bit $Padding_S$. The third part is the $Route\_Sec_S = E(TPK, ID_S||P_S||K_{SD}||Route\_Sec_0\ ||Sign_S(\mathrm{H}(*)))$. User *S* uses *TPK* to encrypts User S' real identity, the pseudonym P_S, session key K_{SD} which is randomly generated by User *S*, $Route\_Sec_0 = \{ID_D||\ Padding_S\}$. User *S* hashes above three parts and encrypts these with its broadcast key K^b_S. Finally User *S* broadcasts $ARREQ_s$ and records $\{TPK||ID_S||\ ID_D||P_S||K_{SD}\}$ secretly.

User *j* received the $ARREQ_i$ from its neighbor User *i*, User *j* first decrypts and check the freshness of the $ARREQ_i$ by compare the *TPK*. Then User *j* uses its private key SK_j to decrypts "$E(PK_D,\ ID_D||TSK||PL_S)$" and checks the destination is itself or not. If User *j* isn't the destination, he generates pseudonym P_j and corresponding session key K_{Pj}. User *j* records $\{TPK||ID_i||P_j||K_{Pj}\}$ and generates $Route\_Sec_j = \mathrm{E}(TPK,\ ID_j||P_j||\ K_{Pj}||Route\_Sec_i||\ Sign_j(\mathrm{H}(*)))$ where P_j and K_{Pj} are pseudonym and corresponding session key. User *j* broadcasts the $ARREQ_j = \{\mathrm{E}(K^b_j, TPK||E(PK_D, ID_D||TSK||PL_S)||\ Route\_Sec_j\ ||\ H(*))\}$. When the target destination *D* receives the $ARREQ_n$ from its neighbor User *n*, it first decrypts "$E(PK_D,\ ID_D||TSK||PL_S)$" to retrieve the *TSK* and then uses *TSK* to decrypt $Route\_Sec_j$. User *D* decrypts $Route\_Sec_i$ layer by layer to get User *i*'s pseudonym P_i and its corresponding session key K_{Pi} until retrieve the $Route\_Sec_0$. User D records P_i and its K_{Pi} in $RouteList(=\{P_1||K_{P1}||\ P_2||K_{P2}||\ldots||P_n||K_{Pn}\})$, where P_1 is the pseudonym of the Source *S*'s neighbor and P_n is the pseudonym of Destination *D*'s neighbor. Finally, User *D* launches *anonymous route reply phase* based on *RouteList.*

3.2 Anonymous route reply phase

The target destination, Access point *D*, performs the *anonymous route reply phase* to confirm the route with User *S* based on *RouteList* which has discovered at Subsection 3.1. User D generates the pseudonym P_D and records $\{TPK||ID_D||ID_S||P_D||K_{SD}\}$ secretly. User D generates the $ARREP_S$ and iteratively generates the route reply message for each User *i* on the route as $ARREP_i$ starting from the neighbor P_1 of Source *S* to the neighbor P_n of Destination *D* based on the order of *RouteList*, where $ARREP_0 = ARREP_S$.

$$ARREP_S = \{P_S||E(K_{SD}, TPK||\ P_D||PL_D||\ RouteList||\ Padding_D)||\ MAC(K_{SD},*)\}$$

$$ARREP_i = \{P_i||E(K_{Pi},\ TPK||ARREP_{i-1})||MAC(K_{Pi},*)\}$$

Finally, User *D* broadcasts $ARREP_n = \{P_n||E(K_{Pn},\ TPK||\ ARREP_{n-1}\ )||\ MAC(K_{Pn},*)\}$.

User j retrieves K_{Pj} from its record $\{TPK||ID_i||P_j||K_{Pj}\}$ based on P_j to verify and decrypts $ARREP_j$ which is broadcasted by its neighbor User k. User j learns it is the source user, if TPK of decrypted $ARREP_j$ is its belongings. User j retrieves and records the pseudonym P_D and *RouteList* from decrypted $ARREP_j$ (= $ARREP_S$). If TPK in $ARREP_j$ is not User j's belongings, User j updates $\{TPK||ID_i||P_j||K_{Pj}\}$ to $\{TPK||\ ID_i||ID_k||P_j\ ||K_{Pj}\}$ and forward the $ARREP_i$ to User i.

4 Performance evaluation

The proposed concept of anonymous secure routing protocol in Section 3 establishes a route based on the proposed *neighbor discovery concept* of Section 2. Each user performs the proposed *neighbor discovery concept* to discover all neighbors considering symmetric and asymmetric communication models. The anonymous secure routing protocol based on the proposed concept establishes a route considering both symmetric and asymmetric communication models while most prior secure/anonymous routing protocols for WMNs did not consider the asymmetric communication model. This section describes the network performance improvement of the proposed concept. Later subsections compare the neighbor discovery rate, success rate for route establishment and the average route hop count between the symmetric model (*i.e*. most of prior secure/anonymous routing protocols for WMNs) and the proposed concept which considers both symmetric and asymmetric communication models. These simulations set the network area as 2 kilometer × 2 kilometer. Users were distributed randomly in the network. The user destinies of simulations are from 1 user / (80 meter × 80 meter) to 1 user / (120meter × 120meter). The simulations classified the user into two kinds: a user with a larger communication range 250 meters called power user and a user with a smaller communication range 125 meters called a normal user.

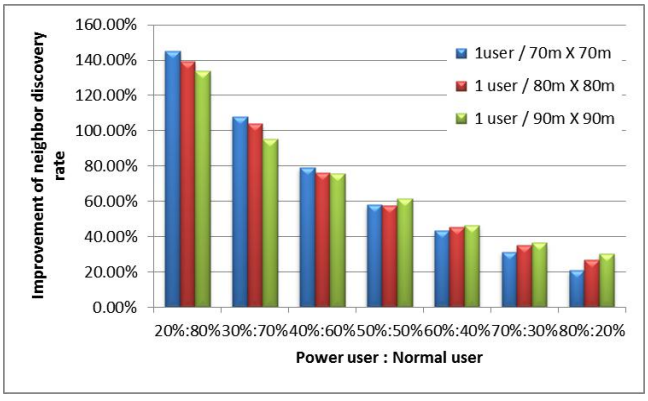

Figure 2. Improvement of neighbor discovery rate of Normal user

4.1 Improvement of neighbor discovery rate

This subsection discusses the neighbor discovery rate improvement by the proposed concept considering both symmetric and asymmetric communication. The simulation measures how many neighbors are discovered by each user in the symmetric model only v.s. the proposed concept. Figure 2 shows the neighbor discovery rate improvement by the proposed concept. If 80% of the users are normal users, the neighbor discovery rate improvement is at least 130%. If the number of power user is larger, *i.e*. more users hold larger communication range, the improvement benefits are smaller. However, the neighbor discovery rate of the proposed concept provides at least 20% improvement when the percentage of normal user decreases to 20%.

4.2 The average route hop count and route establishment success rate

Section 3 proposed a concept of anonymous routing protocol. This concept can be applied to both symmetric and asymmetric models. The user performs the proposed concept to establish a route to the access point with regular-neighbors and semi-neighbor discovered using the *neighbor discovery phase* as detailed in Section 2. This subsection evaluates the efficiency of Data forwarding. These simulations set the hop counts at 10 and 15. Each simulation chooses 20% normal users and 20% power users randomly to establish a route to the Access point. The access point is located at the center of the network. Figure 3 and Figure 4 illustrate comparisons with the average number of hops. The proposed concept establishes a shorter route. The average length of the route established by the proposed concept is 85%~90% of the average route length of routes considering symmetric model only. Even when the number of normal users deceases the proposed concept still finds shorter routes.

Figure 5 and Figure 6 illustrate the comparisons of successful rate with route establishment between different hop count limitations. More users will establish an anonymous secure route to Access point using the proposed concept in comparison with the symmetric model with different hop count limitations. The results demonstrate that the proposed concept establishes more and shorter routes in WMNs.

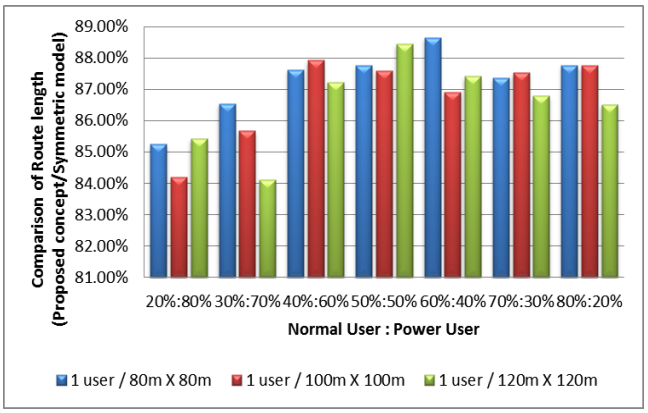

Figure 3. The average hop count of route (hop count = 10)

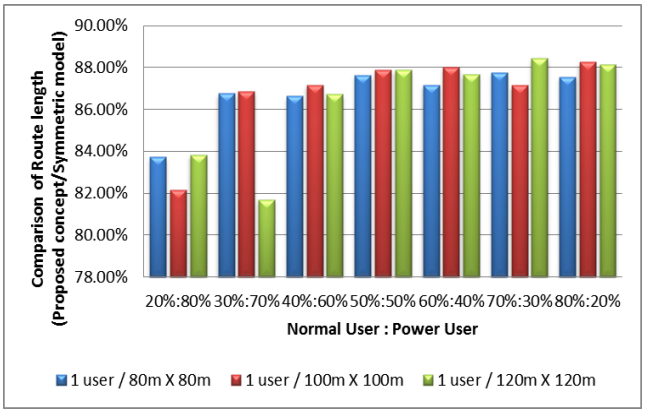

Figure 4. The average hop count of route (hop count = 15)

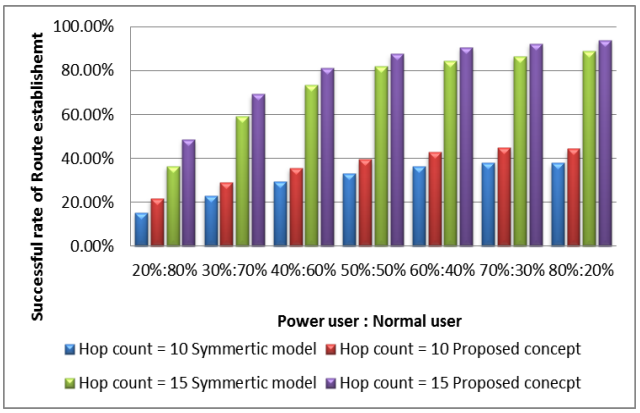

Figure 5. Comparison of route establishment success rate (User Density= 1 user/ 90m × 90m)

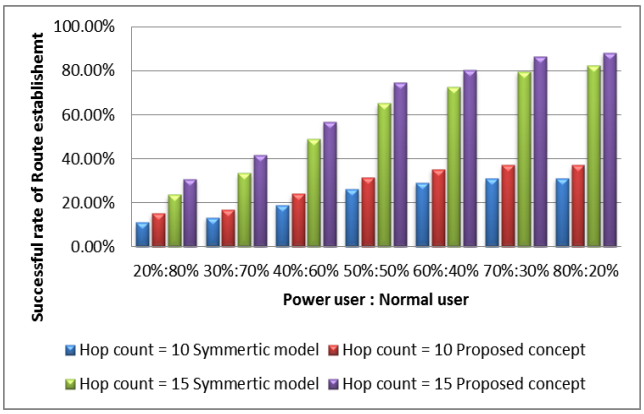

Figure 6. Comparison of route establishment success rate (User Density= 1 user/ 110m × 110m)

5 Conclusions

Anonymity is a very important feature of Wireless Metropolitan Networks security. This paper proposed concepts of anonymous secure routing protocol with asymmetric communication consideration. The proposed concept ensures both the anonymity and security of the routing protocol. This paper firstly proposed a concept of neighbor discovery beyond symmetric and asymmetric models. Each user will identify as many neighbors as possible in its communication range via the proposed neighbor discovery concept. This allows the user to obtain more resources from his neighbors. A wireless device out of the wireless transmission range of the access point may perform the routing protocol based on the proposed concepts to discover a secure route to the access point anonymously. Therefore, more users can obtain the network service and protect their privacy. The proposed concept establishes a shorter route with a higher route establishment success rate because it considers both symmetric and asymmetric models. The anonymous routing protocol based on the proposed concepts is more efficient and suitable for wireless metropolitan networks.

Acknowledgements

This work was partially supported by the National Science Council, Taiwan, under grants no. NSC99-2221-E-032-048.

Reference

[1] Azzedine Boukerche, Khalil El-Khatib, Li Xu, Larry Korba, An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks, Computer Communications, Volume 28, Issue 10, Performance issues of Wireless LANs, PANs and ad hoc networks, 16 June 2005, Pages 1193-1203,

[2] Yigal Bejerano, Seung-Jae Han, Amit Kumar, Efficient load-balancing routing for wireless mesh networks, Computer Networks, Volume 51, Issue 10, 11 July 2007, Pages 2450-2466

[3] Jing Deng, Richard Han, Shivakant Mishra, INSENS: Intrusion-tolerant routing for wireless sensor networks, Computer

Communications, Volume 29, Issue 2, Dependable Wireless Sensor Networks, 10 January 2006, Pages 216-230,

[4] Ying Dong, Tat Wing Chim, Victor O.K. Li, S.M. Yiu, C.K. Hui, ARMR: Anonymous routing protocol with multiple routes for communications in mobile ad hoc networks, Ad Hoc Networks, Volume 7, Issue 8, Privacy and Security in Wireless Sensor and Ad Hoc Networks, November 2009, Pages 1536-1550,

[5] Jakob Eriksson; Michalis Faloutsos; Srikanth V. Krishnamurthy; , "DART: Dynamic Address RouTing for Scalable Ad Hoc and Mesh Networks," Networking, IEEE/ACM Transactions on , vol.15, no.1, pp.119-132, Feb. 2007

[6] Tingyao Jiang, Qinghua Li, and Youlin Ruan. 2004. Secure Dynamic Source Routing Protocol. in Proceedings of the The Fourth International Conference on Computer and Information Technology (CIT '04), Washington, DC, USA, Pages 528-533.

[7] Frank Kargl, Alfred Geis, Stefan Schlott, and Michael Weber. 2005. Secure Dynamic Source Routing. In Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences - Volume 09 (HICSS '05), Vol. 9, Washington, DC, USA,

[8] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. 2003. Rushing attacks and defense in wireless ad hoc network routing protocols. In Proceedings of the 2nd ACM workshop on Wireless security (WiSe '03), New York, NY, USA, Pages 30-40.

[9] Jihye Kim, Gene Tsudik, SRDP: Secure route discovery for dynamic source routing in MANETs, Ad Hoc Networks, Volume 7, Issue 6, August 2009, Pages 1097-1109.

[10] L.A.Martucci, A.Zuccato, S.Fischer-Hübner. Identity Deployment and Management in Wireless Mesh Networks. In: The Future of Identity in the Information Society - Proceedings of the 3rd IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School. Springer. Aug. 2007. Karlstad, Sweden. Pages.223-234.

[11] Rosa Mavropodi, Panayiotis Kotzanikolaou, Christos Douligeris, SecMR - a secure multipath routing protocol for ad hoc networks, Ad Hoc Networks, Volume 5, Issue 1, January 2007, Pages 87-99,

[12] Krichene, N.; Boudriga, N.; , "Intrusion Tolerant Routing for Mesh Networks," 2007 IFIP International Conference on Wireless and Optical Communications Networks, 2-4 July 2007, Singapore, Pages 1-7.

[13] Nagesh S. Nandiraju; Deepti S. Nandiraju; Dharma P. Agrawal; , "Multipath Routing in Wireless Mesh Networks," 2006 IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), Vancouver , Canada, Pages 741-746, 9-12 Oct. 2006.

[14] Ronggong Song, Larry Korba, and George Yee. 2005. AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks. In Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN '05), New York, NY, USA, Pages 33-42.

[15] Ming-Yang Su, WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks, Computers & Security, Volume 29, Issue 2, March 2010, Pages 208-224,

[16] Zhiguo Wan; Kui Ren; Bo Zhu; Preneel, B.; Ming Gu; , "Anonymous User Communication for Privacy Protection in Wireless Metropolitan Mesh Networks," IEEE Transactions on Vehicular Technology , vol.59, no.2, Pages.519-532, Feb. 2010

[17] Jianliang Zheng, Myung J. Lee, A resource-efficient and scalable wireless mesh routing protocol, Ad Hoc Networks, Volume 5, Issue 6, August 2007, Pages 704-718.