# Trust-Aware Anonymous and Efficient Routing for Mobile Ad-Hoc Networks

Min-Hua Shao and Shin-Jia Huang

Department of Management Information Systems, National Pingtung University of Science & Technology, 1 Hseuh Fu Road, Nei Pu, Pingtung, Taiwan 91201

**Abstract.** Anonymous routing is a value-added technique used in mobile ad hoc networks for the purposes of security and privacy concerns. It has inspired lot of research interest, but very few measures exist to trust-integrated cooperation for reliable routing. This paper proposes an optimistic routing protocol for the betterment of collaborative trust-based anonymous routing in MANET. The key features of our scheme are including of accomplishment of anonymity-related goals, trust-aware anonymous routing, effective pseudonym management and lightweight overhead in computation, communication and storage.

## 1 Introduction

Routing security is a paramount concern in MANET and solutions to the routing security have been addressed. In which, anonymous routing is used for the purpose of security and privacy concerns. Anonymity protection in MANET is one of the countermeasures against the mounting intrusions and attacks, such as traffic analysis, spoofing, and denial of service attacks. As discussed in [5,6,7], the following set of anonymity properties investigated into the requirements for MANET are incorporated and extended: (1) *Identity privacy*: No one but the communicating parties can know themselves (the identities of the source and the destination); and further, a node forwarding packets cannot be identified by its neighbors. The former is also named as *source anonymity* and the latter is called as *sender and recipient anonymity*. (2) *Route/path anonymity*: Anyone, either en route or out of the route, cannot infer the identities of intermediaries on a path. (3) *Topology/location privacy*: No one can deduce the arrangement or mapping of the elements (links, nodes, distance, etc.) of a network, from routing information in the packets.

In academic literature, there is often the use of onion routing approach to achieve anonymity goals. ANODR proposed by Kong and Hong [2] is one of the leading proposals to tackle route anonymity and location privacy. The design of ANODR is based on broadcast with trapdoor information. Zhu et al. [7] indicated that their work has more or less weakness and/or security flaws with result that they cannot provide the features and security as claimed. Due to the betterment of privacy and anonymity protection, a solution on anonymity, especially identity anonymity and strong location privacy, is given in Zhu et al.'s work. More recent studies have focus on efficient anonymous routing schemes in MANET. AnonDSR [4], ARM [3] and Discount-

Shao M. and Huang S. (2008).
Trust-Aware Anonymous and Efficient Routing for Mobile Ad-Hoc Networks.
In *Proceedings of the 6th International Workshop on Security in Information Systems*, pages 132-137
DOI: 10.5220/0001731201320137

ANODR [6] are examples. Previous research efforts yielded elegant but typically inefficient solutions to the purpose of trust-aware anonymity. Each mobile node can conduct an anonymous communication with each other in concert with trustworthy intermediaries. In this paper, we propose a trust-based anonymous routing scheme for MANET. In which, the communicating parties can select the most reliable route based on trust management system and feedback the connection experience to the system. The security works about these are essentially different approaches to achieve the same purpose. Besides, an efficient routing protocol that has both strong security and high network performance is considered.

## 2 Notation

The model and all cryptographic symbols for operations are summarized below. (1) *S, D,* $N_x$: *S* is the source node, *D* is the destination node, and $N_x$ is the intermediate nodes. (2) $ID_x$: The real identity of node *x*. (3) $F_x$: The flag is used to indicate the type of a packet, including of $F_{RREQ}$, $F_{RREP}$, and $F_{DATA}$. (4) *Seq*: In addition to replay attacks, it can uniquely identify the particular message when taken in conjunction with the preceding node's one-time pseudonym. (5) $r_i, q_i$ : Random numbers generated by node *i* are used for the generation of one-time pseudonym. (6) $K_{SD}(\cdot)$ : A symmetric encryption function with the shared secret key $K_{SD}$ between *S* and *D*. (7) $(\overline{pk}, \overline{sk})$ : A one-time public-private key pair is used for the purpose of anonymity. (8) $\overline{pk}\{\cdot\}$ : An asymmetric encryption function using the public key $\overline{pk}$ . (9) $h_x = H(\cdot)$ : A collision resistant one-way hash function $H(\cdot)$ and its result $h_x$ is computed by node *x*. (10) $h_{K_x} = H_{K_x}(\cdot)$ : Keyed hash function using the secret key $K_x$.

## 3 The Proposed Scheme

We assume that a shared secret key $K_{SD}$ existed in between *S* and *D*. Node *S* needs to maintain a list of pairs $(ID_i, K_{si})$ for correspondent nodes. The permanent identity of every node in the network is known by communicating nodes. The proposed protocol consists of the anonymous route discovery and the data transmission.

### 3.1 Trust-aware Anonymous Route Discovery Protocol

The anonymous route discovery process is initiated whenever source node *S* needs to communicate with destination node *D* in secret. In which, the reverse path formation is along with broadcasting a route request (RREQ) packet from *S* to neighbors, as well as the forward path setup will accompany the transmission of the eventual route reply (RREP) packet from *D* to neighbors. Specifically, every node is in possession of three identities for one link, including the real identity and two pseudonyms used in the reverse path and in the forward path respectively.

### A. RREQ Phase

**Step 1.** $S \rightarrow * : \langle F_{RREQ}, Seq, h_{K_{SD}}, \overline{pk}, K_{SD}(r_s, seq, \overline{sk}), \overline{pk}\{ID_s\}, h_s \rangle$

*S* generates the masked identity of *D* by computing $h_{K_{SD}} = H_{K_{SD}}(ID_D)$ of *D*'s real identity with $K_{SD}$. Then, *S* randomly selects one-time key pair $(\overline{pk}, \overline{sk})$ for the establishment of a protected path onion $\overline{pk}\{ID_s\}$. Random number $r_s$ is created for the purpose of pseudonym and also works as a message ID for the validation of the reply *RREP* later. Accordingly, $r_s$ must be unique until the termination of its corresponding *RREQ*. Due to anonymity, *S* produces its pseudonym $h_s = H(ID_s, r_s)$ and then *S* computes $K_{SD}(r_s, seq, \overline{sk})$ that is intended for *D*, maintains the associated data in the route table, and broadcasts the *RREQ* packet to its own neighbors.

**Step 2.** $N_x \rightarrow * : \langle F_{RREQ}, Seq, h_{K_{SD}}, \overline{pk}, K_{SD}(r_s, seq, \overline{sk}), \overline{pk}\{\overline{pk}\{ID_s\}ID_x, r_x\}, h_x \rangle$

$N_{x+1} \rightarrow * : \langle F_{RREQ}, Seq, h_{K_{SD}}, \overline{pk}, K_{SD}(r_s, seq, \overline{sk}), \overline{pk}\{\overline{pk}\{\overline{pk}(ID_s\}ID_x, r_x\}ID_{x+1}, r_{x+1}\}, h_{x+1} \rangle$

$N_{x+n} \rightarrow * : \langle F_{RREQ}, Seq, h_{K_{SD}}, \overline{pk}, K_{SD}(r_s, seq, \overline{sk}), \overline{pk}\{\ldots\{\overline{pk}\{\overline{pk}\{\overline{pk}\{ID_s\}ID_x, r_x\}ID_{x+1}, r_{x+1}\}\ldots\}ID_{x+n}, r_{x+n}\}, h_{x+n} \rangle$

Upon receiving the packet, node $N_x$ firstly checks whether it is the concerned node. It calculates $h_{K_{ix}} = H_{K_{ix}}(ID_x)$ for each correspondent node *i* in the list of pairs $(ID_i, K_{ix})$. Here, we assume that $N_x$ is one of intermediate nodes. When the verification doesn't hold, it uses the pair $(seq, h_{x+n-1})$ as a key to search its route table. If a match is found, $N_x$ drops the redundant *RREQ* and does not rebroadcast it. Otherwise, $ID_x$ and $r_x$ randomly generated are appended to the cryptographic onion $\overline{pk}\{\overline{pk}\{ID_s\}ID_x, r_x\}$ by using $\overline{pk}$. $N_x$ computes its pseudonym $h_x = H(h_s, ID_x, r_x)$ and replaces $h_s$ with $h_x$ as a forwarder. Lastly, $N_x$ keeps the routing information in the table and rebroadcasts the *RREQ*. The variation of the *RREQ* packet among intermediate nodes is depicted in the step 2.

**Step 3.** *D receives the RREQ packet.*

The check of the destination is similar to the beginning of step 2. Suppose that *D* can find $h_{K_{iD}} = H_{K_{iD}}(ID_D) = h_{K_{SD}}$ from the list of pairs $(ID_i, K_{iD})$ and use the key $K_{SD}$ to decrypt the ciphertext $K_{SD}(r_s, seq, \overline{sk})$. A protected path $\{ID_s, ID_x, ID_{x+1}, \ldots, ID_{x+n}\}$ is restored by peeling the onion off gradually with $\overline{sk}$. *D* uses the chain of ( $ID_i$, $r_i$ ) for all nodes en route to verify the authenticity of the pseudonym $h_{x+n}$ by computing $H(\ldots(H(H(H(ID_s, r_s), ID_x, r_x), ID_{x+1}, r_{x+1})\ldots), ID_{x+n}, r_{x+n})$, and rejects the packet if the verification is failed. This is used to ensure that the anonymous link on the reverse path corresponds to the real link received. *D* maintains the route table. It is clear that there may be more than one path received, if *D* has already received a *RREQ* with the same pair $(seq, h_{x+n})$. After the reasonable waiting time is ended, *D* may select the most trustable path or the shortest path from the table and make ready for the *RREP*.

**B. RREP Phase**

**Step 1.** $D \rightarrow *:< F_{RREP}, Seq, h_{x+n}, K_{SD}(q_D, chain(r_i), chain(ID_i), Seq), h_D >$

Due to privacy concerns, the destination node *D* randomly generates a number *q* and produces its pseudonym $h_D = H(ID_D, q_D)$ used in the forward path for the *RREP*. The path information and other items $(r_s, q_D, seq)$ are encrypted by the shared key $K_{SD}$. The value $chain(r_i) = \{r_s, r_x, r_{x+1},.., r_{x+n}\}$ is the set of random number $r_i$ generated by all involved nodes, that is, $chain(ID_i) = \{ID_s, ID_x, ID_{x+1},.., ID_{x+n}, ID_D\}$ . *D*, then, unicasts the *RREP* to its specific neighbor $h_{x+n}$, that is, the next node of *D* in the reverse path.

**Step 2.** $N_{x+n} \rightarrow *: \langle F_{RREP}, Seq, h_{x+n-1}, K_{SD}(q_D, chain(r_i), chain(ID_i), Seq), \bar{h}_{x+n} \rangle$

$N_{x+1} \rightarrow *: \langle F_{RREP}, Seq, h_x, K_{SD}(q_D, chain(r_i), chain(ID_i), Seq), \bar{h}_{x+1} \rangle$

$N_x \rightarrow *: \langle F_{RREP}, Seq, h_s, K_{SD}(q_D, chain(r_i), chain(ID_i), Seq), \bar{h}_x \rangle$

The receiving node $N_{x+n}$ firstly compares $h_{x+n}$ with its identity for each pseudonym in the route table and discards the packet if no match is found. Otherwise, if the pseudonym of next node in the reverse path is not filled with "*null*" in the matched entry, node $N_{x+n}$ retrieves $r_{x+n}$ used in the *RREQ* from the route table and generates a new pseudonym $\bar{h}_{x+n}$ by computing $\bar{h}_{x+n} = H(h_D, ID_{x+n}, r_{x+n})$ in order to keep anonymity on the forward path. The next node of $N_{x+n}$ in the forward path is $h_D$. Afterwards, node $N_{x+n}$ replaces $h_D$ with $\bar{h}_{x+n}$ and unicasts the *RREP* back to $h_{x+n-1}$. The treatment of the *RREP* among intermediate nodes is listed above.

**Step 3.** *S receives the packet.*

Assume that node *S* has the same pseudonym $h_s$ appeared in the route table and the pseudonym of next node in the reverse path is filled with "*null*" in the matched entry. The *RREP* travels back to the source. *S* retrieves the shared secret key $K_{SD}$ to obtain the list of real identities on the path. In order to assure the validity of the forward path, *S* compares the received item $\bar{h}_x$ with the new one from the computation of $H(H(...(H(H(ID_D,q_D),ID_{x+n},r_{x+n}),...),ID_{x+1},r_{x+1}),ID_x,r_x)$ , and aborts if the verification doesn't hold. Otherwise, $\bar{h}_x$ is assigned to the pseudonym of next node in forward path for the relevant entry of route table. Because of the end of the forward path, the value of its pseudonym used in forward path is assigned with "*null*". To this end, an anonymous bi-direction link is built and trusted by the communicating parties.

### 3.2 Trust-aware Anonymous Data Transmission Protocol

After an anonymous route is establishment, the DATA transmission protocol will be launched. Its format is as follows, $\langle F_{DATA}, Seq, K_{SD}(DATA, Seq), Anon.ID_{NextHop} \rangle$ . The purpose and process of most fields in the DATA are similar to the RREQ and the RREP. Specifically, the treatment of $Anon.ID_{NextHop}$ is the key to fulfill data forwarding. Note that the distinction of data forwarding in the bi-direction link is marked "*a*" for the forward path and "*b*" for the reverse path.

**Step 1a.** $S \rightarrow * \langle F_{DATA}, Seq, K_{SD}(DATA, Seq), \overline{h}_x \rangle$

**Step 2a.**

$N_x \rightarrow * : \langle F_{DATA}, Seq, K_{SD}(DATA, Seq), \overline{h}_{x+1} \rangle$

$N_{x+1} \rightarrow * : \langle F_{DATA}, Seq, K_{SD}(DATA, Seq), \overline{h}_{x+n-1} \rangle$

$N_{x+n} \rightarrow * : \langle F_{DATA}, Seq, K_{SD}(DATA, Seq), h_D \rangle$

**Step 3a.** *D receives the packet.*

**Step 1b.** $D \rightarrow * \langle F_{DATA}, Seq, K_{SD}(DATA, Seq), h_{x+n} \rangle$

**Step 2b.**

$N_{x+n} \rightarrow * : \langle F_{DATA}, Seq, K_{SD}(DATA, Seq), h_{x+n-1} \rangle$

$N_{x+1} \rightarrow * : \langle F_{DATA}, Seq, K_{SD}(DATA, Seq), h_x \rangle$

$N_{x+n} \rightarrow * : \langle F_{DATA}, Seq, K_{SD}(DATA, Seq), h_s \rangle$

**Step 3b.** *S receives the packet.*

## 4 Discussions

We firstly show how realization of privacy concerns is achieved in the proposed scheme. Then, some features related to practicability and effectiveness are discussed.

**Anonymous Analysis.** The real identities of *S* and *D* are kept secret by the hash operation $h_s = H(ID_s, r_s)$ and $h_D = H(ID_D, q_D)$. Similarly, the intermediaries en route generate the one-time pseudonyms by using the same way to conceal their identities from all nodes, except the communicating parties. This is for the purpose of trust-aware routing. Every intermediary is in possession of two pseudonyms $h_i$ and $\overline{h}_i$ on the bi-direction link. A node receiving, sending, or forwarding packets cannot be identified by its neighbors or inferred the identities of other nodes, either en route or out of the route. No routing information about the exact location, the distance and the true routing path of *S* and *D* is appeared in or deduced from the packets.

**Trust-aware Anonymous Routing.** An anonymous routing based on collaborative effort of trust management systems is considered. In our scheme, *D* can know the identities $chain(ID_i) = \{ID_s, ID_x, ID_{x+1}, .., ID_{x+n}, ID_D\}$ of the intermediaries en route for all RREQ packets received. *D* can select the most reliable route from them according to trust value and *S* may also abort the route if any untrusted node is involved. *S* and *D* can feedback the communicating experience to trust systems.

**Pseudonym Management.** Our method of lowering the computational overhead and identifier management is one-time identifier that mades up from $h_i = H(..(H(ID_s, r_s)..), ID_i, r_i)$ and $\overline{h}_i = H(..(H(ID_D, q_D)..), ID_i, r_i)$. They are generated as receiving the *RREQ* and the *RREP*, rather than pre-establishment. It is effective to achieve unlinkability and practicable to work in MANET with constrained capability.

**Lightweight Overhead.** The detection of the final destination is the key effect on performance. In our scheme, a keyed-Hash Message Authentication Code $h_{K_{SD}} = H_{K_{SD}}(ID_D)$ is used in the *RREQ* in order to check whether *D* is reached. HAMC should execute in approximately the same time as the embedded hash function. It's time complexity of matching computations is acceptable in MANET. The burden of decryption operations has been only put on the communicating parties rather than on nodes en route. The treatment is reasonable because they are willing to take on heavy loading. In addition, terminating condition is required for reducing communication overhead. The pair $(seq, h_{x+n-1})$ uniquely identifies a RREQ, and the combinations of related pseudonyms can determine the end of the RREP and the DATA.

## 5 Conclusions

Within the wireless networks an anonymous routing protocol toward security and privacy concerns is very promising. This is a supplement to current MANET systems and applications, which are much more vulnerable to malicious exploits than conventional wired and the fixed backbone wireless networks. In this paper, we have shown efficient solutions to trust-aware anonymity for the route discovery and hence for subsequent data forwarding using the route. Considering many of early studies remove important performance optimizations, the proposed scheme can provide a better tradeoff between security and performance.

## Acknowledgements

This research was funded by the National Science Council of Taiwan under the contract of NSC 96-2416-H-020-002-MY2.

## References

1. Hegland, A.M., Winjum, E., Mjolsnes, S.F., Rong, C., Kure, O., Spilling, P.: A survey of key management in ad hoc networks. IEEE Communications Surveys & Tutorials, Vol. 8, No. 3. (3rd Quarter 2006) 48 - 66
2. Kong, J., Hong, X.: ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks. Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing. (June 2003) 291 - 302
3. Seys, S., Preneel, B.: ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks. 20th International Conference on Advanced Information Networking and Applications, Vol. 2. (18-20 Apr. 2006) 133 - 137
4. Song, R., Korba, L., Yee, G.: AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks. SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks. (Nov. 2005) 33 – 42.
5. Sy, D., Chen, R., Bao, L.: ODAR: On-demand anonymous routing in ad hoc networks. IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS). (Oct. 2006) 267 - 276
6. Yang, L., Jakobsson, M., Wetzel, S.: Discount anonymous on demand routing for mobile ad hoc networks. Securecomm and Workshops. (2006) 1 – 10
7. Zhu, B., Wan, Z., Kankanhalli, M.S., Bao, F., Deng, R.H.: Anonymous secure routing in mobile ad-hoc networks. 29th Annual IEEE International Conference on Local Computer Networks. (16-18 Nov. 2004) 102 - 108