Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.207 – 211

RESEARCH ARTICLE

Secure Protocol for MANET based on Pseudonomity

S.Chidambaranathan
Head, Department of MCA, St. Xavier's College (Autonomous), Tirunelveli, India
scharan2009@rediffmail.com

Abstract— Adhoc networks that require strong privacy need private routing, which is still a very big challenge. For this sake, so many methodologies have been proposed to address the privacy requirement of adhoc networks. Though, no single methodology can support unlinkability, anonymity in a full-fledged manner. In this work, we concentrate on pseudonomity which ensures high degree of anonymity and unlinkability. This in turn provides strong privacy. Thus, the user is protected against attackers. Experimental results show that our proposed method shows a remarkable degree of privacy when compared to the existing methodologies.

Keywords— Adhoc networks, anonymity, pseudonomity, privacy

I. INTRODUCTION

Privacy preservation is the major concern in mobile adhoc networks rather than wired networks. The reason is that the users will be in moving state and not static, hence there are more chances for security breaches. Problems related to privacy can easily be treated for wired networks, since all the matters taking place are static. Also, mobility pattern is not needed to be treated.

In communication networks, we have a popular terminology or notion with response to privacy preservation. They are anonymity, unlinkability, unobservability and pseudonomity. So far, the term pseudonomity had not been considered in any existing work.

All these notions are defined and are briefly discussed in [15]. All the definitions are given below and are based on Item of Interest(IoI).

Anonymity- Anonymity is the state of being not identifiable within a set of subjects, the anonymity set. The anonymity set is the set of all possible subjects.

Unlinkability- Unlinkability of two or more items of interest (IOIs, e.g., subjects, messages, events, actions.,) means that within the system (comprising these and possibly other items), from the attacker's perspective, these items of interest are no more and no less related after his observation than they are related concerning his a-priori knowledge. This means that the probability of those items being related from the attacker's perspective stays the same before (a-priori knowledge) and after the attacker's observation (a-posteriori knowledge of the attacker).

Unobservability- Unobservability is the state of items of interest (IOIs) being indistinguishable from any IOI (of the same type) at all. Unobservability can be regarded as a possible and desirable property of steganographic systems (see Section 8 "Known mechanisms for anonymity and unobservability"). Therefore it matches the information hiding terminology.

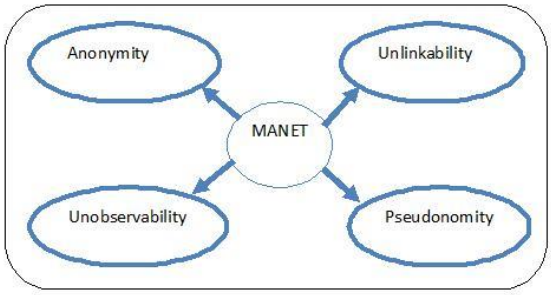

Fig 1: MANET

Pseudonomity- Being pseudonymous is the state of using a pseudonym as ID. Being pseudonymous is the state of using a pseudonym as ID. A digital pseudonym is a bit string and is unique as ID. However, to handle accountability, we follow a scheme that is explained later.

Only by considering all these factors, we can ensure privacy for Mobile adhoc networks. Pseudonomity is the additional parameter that we've used to provide privacy. Most of the existing works concentrate on anonymity and unlinkability.

In our proposed work, we turn our focus also to another parameter, in order to make our system stronger. It is pseudonomity, we use group pseudonyms to safeguard the privacy of mobile adhoc network.

II. RELATED WORK

A number of anonymous routing schemes have been pro- posed for ad hoc networks in recent years, and they provide different level of privacy protection at different cost. Most of them rely on public key cryptosystems (PKC) to achieve anonymity and unlinkability in routing.

Although asymmetry of PKC can provide better support for privacy protection, expensive PKC operations also bring significant computation overhead. Most schemes are PKC-based and the ANODR scheme proposed by Kong et al. [1] is the first one to provide anonymity and unlinkability for routing in ad hoc networks.

Based on onion routing for route discovery, ANODR uses one-time public/private key pairs to achieve anonymity and unlinkability, but unobservability of routing messages is not considered in its design. During the route discovery process, each intermediate node creates a one-time public/private key pair to encrypt/decrypt the routing onion, so as to break the linkage between incoming packets and corresponding outgoing packets. However, packets are publicly labeled and the attacker is able to distinguish different packet types, which fails to guarantee unobservability as discussed. Meanwhile, both generation of one-time PKC key pairs (this can be done during idle time) and PKC encryption/decryption present significant computation burden for mobile nodes in ad hoc networks.

ASR [2], ARM [3], AnonDSR [4] and ARMR [5] also make use of one-time public/private key pairs to achieve anonymity and unlinkability. ASR is designed to achieve stronger location privacy than ANODR, which ensures nodes on route have no information on their distance to the source/destination node. As the routing onion used in ANODR exposes distance information to intermediate nodes, ASR abandons the onion routing technique while still make use of one-time public/private key pair for privacy protection. ARM [3] considered to reduce computation burden on one-time public/private key pair generation. Different from the above schemes, ARMR [5] uses one-time public keys and bloom filter to establish multiple routes for MANETs.

Besides one-time public/private key pairs, SDAR [6] and ODAR [7] use long-term public/private key pairs at each node for anonymous communication. These schemes are more scalable to network size, but require more computation effort. For example, SDAR is similar to ARM except ARM uses shared secrets between source and destination for verification. Unfortunately, ODAR provides only identity anonymity but not unlinkability for MANET, since the entire RREQ/RREP packets are not protected with session keys.

A more recent scheme [8] provides a solution for protecting privacy for a group of interconnected MANETs, but it has the same problem as ODAR. MASK [9] is based on a special type of public key cryp- tosystem, the pairing-based cryptosystem, to achieve anonymous communication in MANET. MASK requires a trusted authority to generate sufficient pairs of secret points and corresponding pseudonyms as well as cryptographic parameters. Hence the setup of MASK is quite expensive and may be vulnerable to key pair depletion attacks.

The RREQ flag is not protected and this enables a passive adversary to locate the source node. Moreover, the destination node's identity is in clear in route request packets. Though this would not disclose

where and who the destination node is, an adversary can easily recover linkability between different RREQ packets with the same destination, which actually violates receiver anonymity as define d in [10].

An anonymous location-aided routing scheme ALARM [11] makes use of public key cryptography and the group signature to preserve privacy. The group signature has a good privacy preserving feature in that everyone can verify a group signature but cannot identify who is the signer. But ALARM still leaks quite a lot sensitive privacy information: network topology, location of every node. Similar to ALARM, PRISM [12] also employs location information and group signature to protect privacy in MANETs.

A closely related research direction along this line is anonymous routing in peer-to-peer systems, which has been investigated heavily too. Interested readers are referred to [13],[14] for details. To summarize, public key cryptosystems have a preferable asymmetric feature, and it is well-suited for privacy protection in MANET. As a result, most anonymous routing schemes proposed for MANET make use of public key cryptosystems to protect privacy.

However, existing schemes provide only anonymity and unlinkability, while unobservability is never considered or implemented by now. An obvious drawback in existing schemes is that packets are not protected as a whole. Information like packet types, trapdoor information, public keys is simply unprotected in current proposals, and these can be exploited by a global adversary to obtain useful information.

III. PROPOSED WORK

In this work, we propose a new protocol exclusively for MANET. Since, we consider mobile adhoc networks intensive care has to be rendered. Here, we focus in achieving accountability too. In our work, every node is supposed to have a pseudonym, so we go for transferable group transaction pseudonym, which induce anonymity set, in which the adversary cannot predict that a particular action has carried out by this particular subject and also the pseudonyms are changed within the subjects then and there.

In order to authenticate pseudonyms, we've identity brokers, who checks for the identity of the subject of t he pseudonym and issues a digitally signed statement that this particular identity broker has proof of the identity of the subject of this digital pseudonym and is willing to divulge that proof under well-defined circumstances.

Whenever a subject involves in any action, the digitally signed statement of a trusted identity broker is checked before entering into any action with the pseudonym's subject, and hence, accountability can be realized in spite of anonymity.

For each action, a pseudonym unlinkable to any other transaction pseudonyms and at least initially unlinkable to any other IOI is used, e.g., randomly generated transaction numbers for online-banking. Therefore, transaction pseudonyms can be used to realize as strong anonymity as possible.

Pseudonyms are public keys generated by the subjects. Some of the main advantages of using pseudonyms are authenticity, validity, revocation if found wrong, reusability since we use transferrable pseudonym.

IV. ALGORITHM/FLOWCHART

Algorithm of the proposed system is presented in Fig 2 and its corresponding flowchart is presented in Fig 3. The algorithm is executed whenever the node is about to perform an action.

```
subject creates pseudonyms;
for every 20 seconds
   transfer pseudonym with another subject;
   end for
check identity of the subject;
 if(fake identity)
  revoke pseudonym;
   else
issue digitally signed statement;
allow subject to perform action;
end if;
end;
```

Fig 2: Algorithm

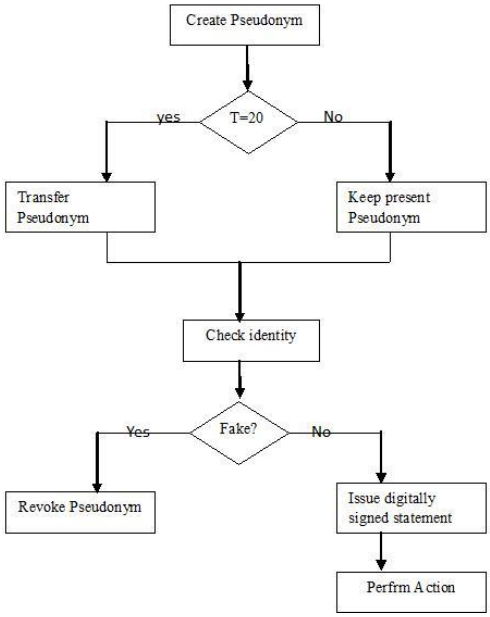

Fig 3: Flowchart of the algorithm

Here, the first half of the algorithm renders anonymity and the second half ensures accountability. Thus, in this work full-fledged security is guaranteed as transferable group transaction pseudonym is used. Reusability, authentication and accountability are ensured with this work. Thus, the security level is considerably increased.

V. CONCLUSIONS

In this work, a new protocol exclusively for the security of MANET has been presented. This is completely based on pseudonym, and we use transferable group transaction pseudonym for better security and can be seen in results. Through this work all security, accountability, authenticity are achieved effectively. In future, this work can be clubbed with the other model for enhanced security.

REFERENCES

[1] J. Kong and X. Hong, "ANODR: aonymous on demand routing with untraceable routes for mobile ad-hoc networks," in Proc. ACM MOBI- HOC'03, pp. 291–302.

[2] B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. KankanHalli, "Anony- mous secure routing in mobile ad-hoc networks," in Proc. 2004 IEEE Conference on Local Computer Networks, pp. 102–108.

[3] S. Seys and B. Preneel, "ARM: anonymous routing protocol for mobile ad hoc networks," in Proc. 2006 IEEE International Conference on Advanced Information Networking and Applications, pp. 133–137.

[4] L. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks," in Proc. 2005 ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 33– 42.

[5] Y. Dong, T. W. Chim, V. O. K. Li, S.-M. Yiu, and C. K. Hui, "ARMR: anonymous routing protocol with multiple routes for communications in mobile ad hoc networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1536 – 1550, 2009.

[6] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks," in Proc. 2004 IEEE LCN, pp. 618–624.

[7] D. Sy, R. Chen, and L. Bao, "ODAR: on-demand anonymous routing in ad hoc networks," in 2006 IEEE Conference on Mobile Ad-hoc and Sensor Systems.

[8] K. E. Defrawy and G. Tsudik, "ALARM: anonymous location-aided routing in suspicious MANETs," IEEE Trans. Mobile Comput., vol. 10, no. 9, pp. 1345–1358, 2011.

[9] El Defrawy, Karim, and Gene Tsudik. "Privacy-preserving location-based on-demand routing in MANETs." Selected Areas in Communications, IEEE Journal on 29.10 (2011): 1926-1934.

[10] J. Han and Y. Liu, "Mutual anonymity for mobile peer-to-peer systems," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 8, pp. 1009–1019, Aug. 2008.

[11] Y. Liu, J. Han, and J. Wang, "Rumor riding: anonymizing unstructured peer-to-peer systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 3, pp. 464–475, 2011.
[12] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Advances in Cryptology– Crypto'04, Lecture Notes in Computer Science, vol. 3152, 2004, pp. 41–55.
[13] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Advances in Cryptology– Crypto'01, Lecture Notes in Com- puter Science, vol. 2139, 2001, pp. 213–229.
[14] D. Dong, M. Li, Y. Liu, X.-Y. Li, and X. Liao, "Topological detection on wormholes in wireless ad hoc and sensor networks," IEEE/ACM Trans. Netw., vol. 19, no. 6, pp. 1787–1796, Dec. 2011.
[15] A. Pfitzmann and M. Hansen, "Anonymity, unobservability, and pseudonymity: a consolidated proposal for terminology," draft, July 2000.

S.Chidambaranathan, received his post graduate degree in Mathematics from Madurai Kamaraj University, Madurai. He also earned post graduate degree in Computer Application and M.Phil in computer Science from Manonmaniam Sundaranar University, Tirunelveli. Presently he is working as HoD in the Department of MCA, St. Xavier's College (Autonomous), Palayamkottai, Tamil Nadu. He is an author for many books including "PHP for beginners", "XML-An Practical approach" and "Everything HTML". He has published many research papers in National, International journals and conference proceedings. He can be contacted at E-mail: scharan2009@rediffmail.com

