Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Privacy Aware Schemes in Mobile Adhoc Networks

Manpreet Singh*, Chakshu Goel, Gurpreet Singh

ECE, SBSSTC, Ferozepur

India

Abstract — A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. Both selfish and privacy issues have been identified as two crucial human factors for the wide acceptance of MANETs. Security has become a primary concern in order to provide protected communication between mobile nodes. In this work we present a review on a number of privacy aware schemes but credit-based incentive and privacy-aware data dissemination (IPAD) scheme for MANETs, which mainly exploits how to simultaneously protect mobile node's privacy and provide a fair incentive for efficiently disseminating a time-valuable data in privacy-aware MANETs provides more privacy.

Keywords— MANETs; Traffic Control; AODV;

I. INTRODUCTION

In recent years, much interest has been involved in the design of Mobile Ad-hoc Network (MANET) technologies. These networks are characterized by their open peer-to-peer network architecture, self-configuration, stringent resource constraints, highly dynamic network topology, and shared wireless medium. These characteristics make them vulnerable to security attacks. Existing security solutions for wired or wireless networks with infrastructure cannot be directly applied to MANETs. The designing security solutions for MANET are the nontrivial challenges. The goal of security solutions is to provide security services like authentication, integrity, availability and confidentiality to mobile users.

The opportunistic network is an extension of Mobile Ad hoc Network (MANET). Wireless networks properties, such as disconnection of nodes, network partitions, mobility of users and links instability, are seen as exceptions in traditional network. This makes the design of MANET significantly more difficult. Opportunistic networks are created out of mobile devices carried by people, without relying on any pre-existing network topology. Opportunistic networks consider mobility, disconnections, partitions, etc. as norms instead of the exceptions. In opportunistic network mobility is used as a technique to provide communication between disconnected groups of nodes, rather than a drawback to be solved.

In opportunistic networking a complete path between two nodes wishing to communicate is unavailable. Opportunistic networking tries to solve this problem by removing the assumption of physical end-to-end connectivity and allows such nodes to exchange messages. By using the store-carry-and-forward paradigm [4] intermediate nodes store messages when there is no forwarding opportunity towards the destination, and exploit any future contact opportunity with other mobile devices to bring the messages closer and closer to the destination.

Opportunistic Networks (OPPNETs), such as delay tolerant networks, vehicular communication networks, and ubiquitous mobile social networks, have received considerable research attention in recent years. As an interesting evolution of MANETs, OPPNETs are more pervasive and distinguishably characterized by non-exist end-to-end connection, but intermittent connectivity among mobile nodes during their opportunistic contacts. However, due to the extremely dynamic and unstable network topology, the packet propagation in OPPNETs usually follows a "store-carry-and forward" manner and the packets can only be opportunistically relayed to their destinations with high transmission delay and low delivery ratio. In order to reduce the transmission delay and increase the delivery ratio, extensive research efforts have recently been put into OPPNET routing and dissemination, and a variety of efficient routing and dissemination protocols [5]–[7], which either rely on network and mobility characteristics or utilize pre-existing social network information, have been proposed for OPPNETs.

Despite the significant progress, selfish and privacy issues, two crucial human factors in OPPNETs, have not been fully exploited in the above protocols, which may make them impractical in real-world OPPNET scenarios. A common hypothesis made in the above protocols is that all nodes are cooperative, i.e., each node is willing to relay packets for others voluntarily.

However, in order to conserve energy, storage and computing resources, some nodes could behave selfishly and will not participate in relaying, which thus violates the hypothesis and makes these well-designed protocols inefficient. To this end, it is imperative to provide some incentive strategies to stimulate selfish nodes to nodal cooperation in OPPNETs [8]. In addition to the selfish issue, privacy issue is also challenging in OPPNETs [9]. If the privacy of node is not well protected, nodes will be still reluctant to participate in nodal cooperation. For example, some protocols study node mobility to improve the network performance, but the node mobility will disclose node's location privacy [10]; other protocols use the pre-existing social network information to accelerate the packet delivery, however the social network information will also depressively release node' identity privacy and social profile privacy. Since huge security and

© 2014, IJARCSSE All Rights Reserved

privacy risks are heavily associated with OPPNETs, how to deal with privacy challenges is crucial for the success of OPPNETs [11].

Although both selfish and privacy issues have been identified as two crucial human factors for the wide acceptance of OPPNETs, many recent research works tend to separately study them in OPPNETs. The reason is that, if the selfish and privacy issues are addressed at the same time in OPPNETs, the problem would become more challenging. For example, some privacy enhanced techniques [12] enable a node to hide its identity and location information, but they could make some incentive strategies, especially the reputation-based incentive strategies, hard to implement in OPPNETs, since a node is no longer identified, and its activities cannot be linked. Therefore, how to simultaneously address selfish and privacy issues becomes particularly challenging in OPPNETs.

II. SECURITY ISSUES IN MOBILE OPPORTUNISTIC NETWORK

Mobile Opportunistic Networks (MobiOpps) are an extreme generalization of Mobile Ad-Hoc Networks (MANETs) that aim at enabling communication between mobile nodes in highly challenged conditions, which raise new networking and security issues due to:

Heterogeneity: as in MANETs, nodes cannot rely on a global infrastructure and on top of that they belong to heterogeneous networks that rely on various communication technologies. This means in particular that naming is an issue, because nodes don't have a unique address across the different networks and furthermore raises the requirement for new authentication and trust establishment mechanisms.

High mobility: nodes are extremely mobile and disruptions in paths are frequent. It is thus impossible to establish a stable end-to-end route: routing and security solutions should be highly dynamic and flexible, and should not depend on a pre-defined path.

Delay tolerance: since nodes belong to heterogeneous networks, an end-to-end path might simply never exist. Messages can still be delivered by adopting a store and forward strategy, where intermediate nodes store messages when communication is impossible and forward them when a communication opportunity arises, for example thanks to mobility. Such a strategy trades a higher delay for a higher delivery ratio, but this also means, from a security point of view, that direct interactions cannot be assumed: end-to-end key agreements are thus unpractical and all protocols relying on an on-line authority need to be revisited.

Because of these characteristics, MobiOpps call for a radical revision of all security aspects of communication, and in the following we present a review of secure routing in Opportunistic Networks.

III. RELATED WORK

Chasaki (2008) in the paper "Topology Reconstruction via Path Recording in Secure MANET" provides a discussion of different path recording mechanisms. They evaluate their performance in terms of packet overhead and reconstruction complexity. The record of the path of a packet through a MANET can be used to validate control plane routing information. Such a mechanism can defend against malicious attempts to disseminating incorrect connectivity information. They explore different methods for recording the identifiers of nodes and links in the network. They consider both deterministic and probabilistic methods and evaluate their performance in terms of space requirements and reconstruction cost. Their evaluation shows the quantitative tradeoffs between these methods.

Luis et al. (2008) in the paper "Securing the communication in Private Heterogeneous Mobile Adhoc Networks" proposed the method a pair-wise key based scheme for forming secured private clusters in mobile adhoc networks. The solution helps to tackles the problem of node authentication combined with traffic encryption in relatively small adhoc networks using proactive neighbour discovery and authentication.

M.A.Matin et al (2009) in the paper "Performance Evaluation of Symmetric Encryption Algorithm in MANET and WLAN" proposed a method on symmetric encryption technique with AES algorithm in MANET and WLAN. Symmetric encryption is faster and requires less computational processing time. By increasing key size as well as block size, the security gets enhanced and linear cryptanalysis and differential cryptanalysis require more time to break the proposed cipher here. S. Thadvai et al. (2012) in the paper "A novel authenticated encryption scheme with convertibility" proposed a method based on message recovery which includes message and the signature hence the communication cost is lower for the message recovery method. In the method they used the Authentication Encryption Scheme (AES) for message recovery.

Shiva et al (2012) in the paper "Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks" proposed the method that the digital signature based secure data transmission in wireless sensor networks. They used the asymmetric key crypto system (public) for the security. MD-5 hash function is used to generate the digital signature. Also RSA algorithm is used which provides digital signature as well as secrecy. The results are compared with AOMDV which is a extension of AODV protocol.

Singh (2013) in the paper "COMPARISON OF AAMRP AND IODMRP USING SBPGP" describes security as major aspect with multicast routing protocol (IODMR and AAMRP). Multicasting is the ability to send packets to and receive packets directed at a subset of nodes in a network. They are applying the SBPGP model with these protocols and will find out their performance under certain conditions with various malicious attacks can be handled efficiently on MANET by using different size of encryption bit keys.

© 2014, IJARCSSE All Rights Reserved

Sameh et al. (2013) in the paper [8] proposes a novel fully distributed and collaborative k-anonymity protocol (LPAF) to protect users' location information and ensure better privacy while forwarding queries/replies to/from un-trusted Location-based Service (LBS) over opportunistic mobile networks (OppMNet). They utilize a lightweight multi-hop Markov-based stochastic model for location prediction to guide queries towards the LBS's location as well as to reduce required resources in terms of retransmission overheads. They develop a formal analytical model and present theoretical analysis and simulation of the proposed protocol performance. They further validate their results by performing extensive simulation experiments over pseudo realistic city-map using map-based mobility models and using real-world data trace to compare LPAF to existing location privacy and benchmark protocols. They show that LPAF manages to keep higher privacy levels and quality of service in terms of success ratio and delay and compared it to other protocols while maintaining lower overheads.

IV. PRIVACY AWARE SCHEMES

IPAD- An Incentive and Privacy-Aware Data Dissemination Scheme: To develop an efficient incentive and privacy-aware data dissemination scheme in OPPNETs to not only accelerate data dissemination in a fair incentive environment but also protect mobile node's privacy IPAD scheme is proposed. It consists of four phases: system initialization phase, data packet generation phase, data packet dissemination phase, and charging and rewarding phase.

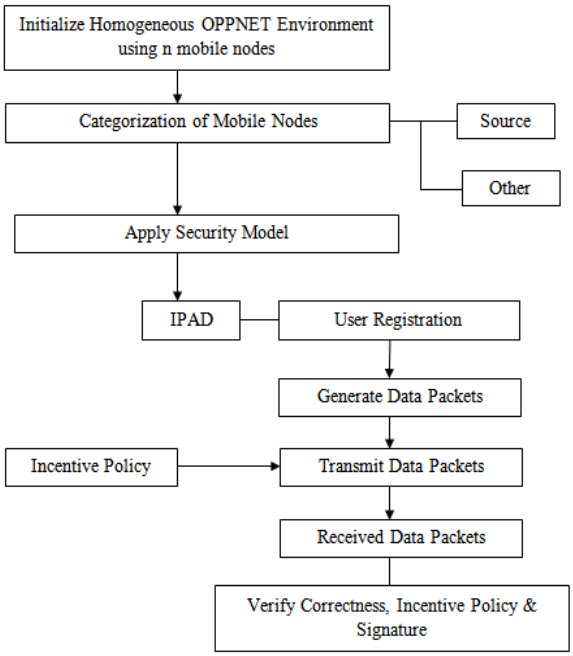

Fig 1: IPAD Scheme

Location Privacy-Aware Forwarding Scheme: A novel fully distributed and collaborative k-anonymity protocol (LPAF) to protect users' location information and ensure better privacy while forwarding queries/replies to/from un-trusted Location-based Service (LBS) over opportunistic mobile networks (OppMNet). The utilization of a lightweight multi-hop Markov-based stochastic model is for location prediction to guide queries towards the LBS's location as well as to reduce required resources in terms of re-transmission overheads.

SPOC- A Secure and Privacy-preserving Opportunistic Computing Scheme: A secure and privacy-preserving opportunistic computing framework SPOC, is for m-Healthcare emergency. With this, smart phone resources including computing power and energy can be opportunistically gathered to process the computing-intensive personal health information (PHI) during m-Healthcare emergency with minimal privacy disclosure. To leverage the PHI privacy disclosure and the high reliability of PHI process and transmission in m-Healthcare emergency, an efficient user-centric privacy access control in SPOC framework is introduced which is based on an attribute-based access control and a new privacy-preserving scalar product computation (PPSPC) technique, which allows a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming PHI data. The Detailed security analysis shows that the proposed SPOC framework can efficiently achieve user-centric privacy access control in m-Healthcare emergency.

V. CONCLUSION

Mobile Ad hoc Networks required security while communication. For example, some privacy enhanced techniques enable a node to hide its identity and location information, but they could make some incentive strategies, especially the reputation-based incentive strategies, hard to implement in MANETs, since a node is no longer identified, and its activities cannot be linked. Therefore, how to simultaneously address selfish and privacy issues becomes particularly challenging in MANETs.

© 2014, IJARCSSE All Rights Reserved

In this paper, we presents a review on a number of privacy aware schemes but credit-based incentive and privacy-aware data dissemination (IPAD) scheme for MANETs, which mainly exploits how to simultaneously protect mobile node's privacy and provide a fair incentive for efficiently disseminating a time-valuable data in privacy-aware MANETs provides more privacy. In IPAD, each node holds a family of unlinkable pseudo-IDs and periodically changes its current pseudo-ID for privacy preservation. When a source node wants to disseminate a time-valuable data to a group of social friends, it also attaches an incentive on the data packet. Then, selfish nodes can be stimulated to participate in relaying to improve the dissemination ratio and reduce the average delay in MANETs.

REFERENCES

[1] Renu Dalal,Yudhvir Singh and Manju Khar, "A Review on Key Management Schemes in MANET" International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2012.
[2] Panagiotis Papadimitratos , Zygmunt J. Haas., "Secure message transmission in mobile ad hoc networks."
[3] Jorg Liebeherr and Guangyu Dong, "An Overlay Approach to Data Security in Ad-Hoc Networks"
[4] Danai Chasaki, Y. Sinan Hanay and Tilman Wolf, "Topology Reconstruction via Path Recording in Secure MANET" 978-1-4244-2677-5/08/$25.00 _c 2008 IEEE.
[5] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Data Transmission in Mobile Ad Hoc Networks" ACM Workshop on Wireless Security (WiSe 2003), San Diego, CA, September 19, 2003.
[6] Abderrezak Rachedi and Abderrahim Benslimane, "A Secure Architecture for Mobile Ad Hoc Networks" International Conference on Mobile Ad-hoc and Sensor Networks (MSN'2006), Hong Kong : China (2006) DOI : 10.1007/11943952_36.
[7] VLADIMIR BERMAN, "Enhancing Data Security in Mobile Ad Hoc Networks via Multipath Routing and Directional Transmission".
[8] Sameh Zakhary, Milena Radenkovic and Abderrahim Benslimane, "Efficient Location Privacy-Aware Forwarding in Opportunistic Mobile Networks".
[9] Rongxing Lu, Xiaodong Lin, Zhiguo Shi, Bin Ca, and Xuemin (Sherman) Shen, "IPAD: An Incentive and Privacy-Aware Data Dissemination Scheme in Opportunistic Networks" 2013 Proceedings IEEE INFOCOM.
[10] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Data Communication in Mobile Ad Hoc Networks" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006.
[11] Kartik Kumar Srivastava, Avinash Tripathi, and Anjnesh Kumar Tiwari, " Secure Data Transmission in MANET Routing Protocol" IJCTA , International Journal ofComputer Technology & Applications,Vol 3 (6), 1915-1921 Nov-Dec 2012.
[12] Danai Chasaki and Tilman Wolf, "Evaluation of Path Recording Techniques in Secure MANET".
[13] Vineetha S. H. and Shebin Kurian, " Performance Analysis of Cluster Based Secure Multicast Key Management in MANET" **I**nternational **J**ournal of **C**omputer **S**cience and **T**elecommunications [Volume 4, Issue 4, April 2013].
[14] Ranjeet Singh, and Prof. Harwant Singh Arri, "COMPARISON OF AAMRP AND IODMRP USING SBPGP" International Journal of Computer Science and Management Research, Vol 2 Issue 3 March 2013.ISSN 2278-733X.
[15] Merin Francis, M. Sangeetha, and Dr. A. Sabari, "A Survey of Key Management Technique for Secure and Reliable Data Transmission in MANET" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013, ISSN: 2277 128X.
[16] I. Parris and T. Henderson, "Privacy-enhanced social-network routing," *Computer Communications*, vol. 35, no. 1, pp. 62–74, 2012.
[17] R. Lu, X. Lin, H. Zhu, X. Shen, and B. R. Preiss, "Pi: a practical incentive protocol for delay tolerant networks," *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1483–1493, 2010.
[18] L. Pelusi, A. Passarella, and M. Conti, "Opportunistic networking: Data forwarding in disconnected mobile ad hoc networks," *IEEE Communications Magazine*, vol. 44, no. 11, pp. 134 – 141, 2006.

© 2014, IJARCSSE All Rights Reserved