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. 8, August 2014, pg.435 – 440

SURVEY ARTICLE

Payment Schemes for Securing Multihop Wireless Networks: A Survey

Mrs.N.Sathya[1], Dr.R.Pugazendi[2]

[1] Department of Computer Science,
K.S.Rangasamy College of Arts and Science,
Tiruchengode, TamilNadu, India

[2] Department of Computer Science,
K.S.Rangasamy College of Arts and Science,
Tiruchengode, TamilNadu, India

[1]sathyanatesan88@gmail.com; [2]pugazendi_r@rediffmail.com

Abstract— A multi-hop wireless network is a network in which a packet traversed in multiple successive wireless links to reach its destination. It is similar to mobile adhoc networks, but nodes in multi-hop wireless network are fixed. Multi-hop wireless networks can be deployed at less lost and it enlarges the coverage area with limited transmit power, enhance the spectral efficiency and network throughput. But the multi-hop wireless networks are vulnerable to different types of attacks. The selfish nodes in the multi-hop wireless networks do not relay other packets and by utilizing the cooperative nodes to transfer the packets to other nodes so that the cooperative nodes are overloaded due to the high traffic. In this survey, several payment schemes are suggested to identify the cheating nodes. The receipt-based payment scheme is one of the schemes in which the accounting center accumulates and organizes the credit account of all the nodes. Each node in the network typically submits indisputable proofs for the relaying packets to the accounting center to update their credit accounts. But the drawback in this method is high communication overhead and computational complexity. Specifically, in this survey different payment schemes are suggested and analyzed the performance.

Keywords: Multi-hop wireless networks, Payment schemes, Network security, Selfishness attacks

I. INTRODUCTION

A Multi-hop wireless network is a wireless network in which the nodes work together in order to provide communication between the nodes. There are more advantages in multi-hop wireless networks. When compared to the single wireless link multi-hop wireless links have more coverage area and increasing network connectivity. Furthermore, by using the multi-hop wireless links there is less transmission power and requires less energy. It ensures high data rates so that achieves high throughput and more efficient in the wireless medium. But the problem in the multi-hop wireless network is that some of the nodes behave in a selfish manner and drop the packets so that there is degradation in network connectivity. In the multi-hop wireless networks, the nodes are eager to spend their limited resources like energy, bandwidth for transmitting packets to other relay nodes. But some of the selfish nodes are not ready to relay packets and by using cooperative nodes to relay the packets so that degradation in the connectivity of the network and fairness.

The following survey has different payment schemes for improving security with less processing overhead. The payment schemes are categorized into two types: One is tamper-proof-device payment scheme and another one is receipt-based payment scheme. A method of credit-card payment schemes is utilized to stimulate the nodes to cooperate in relaying other packets by making cooperation more favourable than selfishness. The nodes in the network earn credits for forwarding the packets and by using these credits to obtain their packets relayed others. But this scheme requires significant processing and high communication overhead and computational complexity. An efficient and secure cooperation incentive method [14] is one of the methods which utilize the public key operations for only the first packet and then hashing operations are used for the next packets. But this method only considers the efficient transmission of messages, but does not consider the overhead problem.

II. RELATED WORKS

In this section, the various payment schemes are suggested and analyzed the performance.

Sergio Marti et.al [1] suggested watchdog to mitigate the routing misbehavior in the mobile adhoc networks. By using this method, there is an only limited change in the routing behavior to detect and reduce the malicious nodes. The dynamic source routing algorithm is recommended to diminish the routing misbehavior: watchdog and pathrater. The watchdog is responsible for discovering the malicious nodes. While, the path rater is responsible for avoiding the routing via the malicious nodes. If a node forwards a packet, the watchdog in the node authenticate the next node and it is given permission to forward the packets. The watchdog carefully listens the next node whether it forwards the packet or not. Suppose, if the next node doesn't forward the packet, it considers as a malicious node. By utilizing the knowledge of the watchdog, the path rater selects the optimal network path.

Sheng Zhong et.al [2] suggested a simple, cheat-proof, credit based method which is called Sprite for motivating cooperation among the selfish nodes in the mobile adhoc networks. Also, this method uses credit for providing incentive to selfish nodes. On the other hand, one of the novel and distinctive features is that the system does not require any tamper-proof hardware at any node.

Luzi Anderegg et.al [3] a truthful and Cost-proficient routing method for Mobile Ad hoc Networks. A game-theoretic setting is used in the mobile adhoc network, which includes of greedy, selfish agents who acknowledge payments for transmitting data for other agents if the payments cover their individual costs acquired by forwarding data. In this setting, a reactive routing method is suggested which accomplishes the design targets of faithfulness and cost-proficiency in a game-theoretic sense by paying to the intermediate nodes a premium over their actual costs for transmitting data packets. The total overpayment is comparatively small by providing a theoretical upper bound and by providing investigational confirmation.

Yanchao Zhang et.al [4] suggested a secure incentive protocol for enhancing security in the multi-hop wireless networks. In this method once a data packet is received, the destination node sends a RECEIPT packet to the source node to provide a REWARD packet to enlarge the credit accounts for the intermediate nodes.

L. Buttyan et.al [5] presented the method which focuses the problem of motivating cooperation in self-organizing in mobile ad hoc networks. In this method, the self-generated and transmitted packets by a node are passed to the tamper-proof device to diminish and enlarge the credit account of the nodes, correspondingly. Packet purse and packet trade methods are suggested. In the packet purse model, the credit account of the source node is charged the full payment before transmitting a packet, and each intermediate node obtains the payment for forwarding the packets to other nodes. In the packet trade method, every intermediate node executes an auction to sell the packets to the next node in the routing path. The destination node pays the total price of relaying the packets.

Kimaya Sanzgiri et.al [6] suggested a technique which is called an authenticated routing method for improving security in adhoc networks. In this work, an adhoc routing method with efficient security is suggested. Firstly, the heterogeneous environments is defined and differentiated which is used to make of ad hoc routing and diverge in their unspecified pre-deployment and security necessities. This method is significant due to satisfying a tighter set of security necessities than an application need is unnecessary and extravagant of resources.

Weyland et.al [7] suggested the CASHnet charging and satisfying mechanism works as follows: Every time a node necessitates transmitting a self-generated packet, or receiving a packet addressed to it, the node has to pay with traffic credits. The amount is either associated with the current distance in hop counts to the gateway or a globally fixed price. Each and every time a node transmits a packet, it obtains helper credits. Traffic credits can be bought for real money or traded for helper credits at service

stations. A service station is comparable to a terminal for loading prepaid cards and has a protected, less bandwidth link to the provider, which is utilized for verification and payment process.

G. F. Marias et.al [8] suggested cooperation enforcement methods for establishing trust model in mobile adhoc networks. The cooperation enforcement scheme is categorized as reputation-based and credit-based schemes are considered for adhoc networks in which the key dissemination centers are transiently present, and for networks that consist of devices with inadequate processing, battery, and memory resources. This Cooperation enforcement method does not present efficient verification of entities. Instead, they give to the recognition of the trustworthiness of peers and to the enforcement cooperation utilizing mutual incentives.

Chao-Chin Chou et.al [9] suggested an anonymous Peer-to-peer Communication Protocol for improving performance in the mobile adhoc networks. This protocol is particularly designed to be a better middleware between the peer-to-peer applications and the routing protocols of the MANET. This protocol utilizes a broadcast-based mechanism and probabilistic-based flooding control mechanism to provide an anonymous path between peer-to-peer applications. There is no necessity for hop-by-hop encryption/decryption consequently it necessitates less computational complexity and power consumption. By using this anonymous Peer-to-peer Communication Protocol, multiple anonymous paths between the peers are established by single query phase and it is highly resilient to malicious attacks.

Jianping Pan Et.al [10] suggested Identity-based secure association method in wireless adhoc networks. In the wireless adhoc networks, the latest technique named as a method of identity-based cryptography is used. Actually, in the public-key cryptography schemes, the certificate authorities stored the identity and public key of the entities. This kind of central authorities is eradicated in the identity-based cryptography method. In this method, the public-key of an entity can be derived from its identity directly. This feature is crucially significant for ad hoc networks, where public-key infrastructures (PKIs) or CA hierarchies are also luxurious to build and susceptible to preserve in general. Identity-based cryptography is used to make possible asymmetric encryption/decryption and signature/verification procedure.

Bachar Wehbi et.al [11] suggested an efficient time synchronization Mechanism for Wireless Multi Hop Networks. The main intent is to design a protocol which synchronizes the network nodes according to one reference node. A connected dominating set is generated by a set of sender nodes for giving guidance for the synchronization process in a multihop network. Every node in the network computes its clock offset and frequency error parameters to build an alteration function that transforms its local time to that of the reference node. This protocol computes the clock offset and the frequency error on dissimilar time scales leading to important gain in terms of synchronization accuracy.

Mohamed Elsalih Mahmoud et.al [12] suggested a method which is called practical incentive system to motivate the support of the nodes in the multi-hop wireless networks. While the communication sessions may arise without concerning an infrastructure, the communicating nodes provide digital receipts for the intermediate nodes, which submit the receipts to the accounting center (AC) to maintain their payment. The decisive point of the practical completion of incentive systems is the receipts' submission and high overhead because of the high frequency of low-value transactions. If there is a huge number of receipts is submitted for the node clarification, there are high computation overhead and high complexity.

Rongxing Lu et.al [13] suggested the practical Incentive Protocol for Delay Tolerant Networks. The cooperative network like DTN and the occurrence of selfish DTN nodes could cause catastrophic injuries to any well intended opportunistic routing design and expose the whole network. To reduce the attack which is caused by the selfish nodes in the delay-tolerant networks a practical incentive protocol is suggested in which a source node transmits a bundle message and also it merges some incentive on the bundle, which is not only elegant but also fair to all contributing DTN nodes. To accomplish good packet delivery ratio, the selfish DTN nodes could be motivated to help with forwarding bundles. Furthermore, this method can also avoid different attacks which could be launched by the selfish nodes.

Mohamed Elsalih Mahmoud et.al [15] suggested a novel mechanism which can prevent the rational and irrational packet dropping attacks by adopting inspiration and punishment strategies (TRIPO). TRIPO utilizes micropayment to motivate the rational packet droppers to relay the others' packets and implement equality and the reputation system is used to recognize and remove the irrational packet droppers. Instead of utilizing the medium eavesdropping technique, a new monitoring technique is suggested for evaluating the nodes frequency of dropping packets according to the processing the payment receipts. The receipts can survive processed to eliminate financial information to recompense the cooperative nodes that relay packets, and also appropriate information, like broken links, to build up the reputation system **(**RS).

Mohamed M.E.A et.al [16] suggested a fair and proficient incentive mechanism to stimulate the collaboration of the nodes. To provide the efficient security at the source and destination nodes, the lightweight hashing processing is used in the ACK packets to diminish the number of public-key-cryptography processes. The destination node creates a hash chain and signs for its root, and acknowledges message response by liberating a hash value from the hash chain. Instead of creating signature per message, the destination node creates a signature per group of messages. Additionally, a small-size check including the payment data for the entire intermediate nodes is generated per route instead of creating a check per message.

TABLE I

ANALYSIS OF METHODS

S.NO	TITLE	AUTHOR	METHODS	MERITS	DEMERITS
1	Mitigating Routing Misbehavior in Mobile Ad Hoc Networks[1]	S. Marti, T. Giuli, K. Lai, and M. Baker	Watch dog mechanism	Increase network throughput.	Does not find the optimal values to increase the throughput
2	Sprite: A Simple, Cheat-Proof, Credit Based System for Mobile Ad-Hoc Networks[2]	S. Zhong, J. Chen, and R. Yang	Sprite, a simple, cheat-proof, credit based System.	Less overhead.	Less secure.
3	Ad hoc-VCG: A Truthful and Cost-Efficient Routing Protocol for Mobile Ad hoc Networks with Selfish Agents[3]	Luzi Anderegg, Stephan Eidenbenz	A Truthful and Cost-Efficient Routing Protocol	High energy efficiency and less overhead.	Does not consider the selfish nodes.
4	SIP: A Secure Incentive Protocol against Selfishness in Mobile Ad Hoc Networks[4]	Yanchao Zhang, Wenjing Lou, Yuguang Fang	Secure Incentive Protocol	Low Overhead.	High computation complexity.
5	Stimulating Cooperation in Self- Organizing Mobile Ad Hoc Networks," Mobile Networks and Applications[5]	L. Buttyan and J. Hubaux	Cooperation Method.	Increase the overall network performance.	Less secure.
6	Authenticated Routing for Ad Hoc Networks[6]	K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer	Authenticated Routing for Ad hoc Networks (ARAN)	Effectively and efficiently discover secure routes.	High latency, high computation.
7	Cooperation and Accounting in Multi-Hop Cellular Networks[7]	A. Weyland	Cooperation and accounting strategy for hybrid networks called CASHnet	Reduce the energy consumption for transmitting packets	Specification of the charging and remuneration relation is not considered.
8	Cooperation Enforcement Schemes for MANETs: A Survey[8]	G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas	Reputation-based and credit-based methods.	High throughput is achieved.	Fairness is not considered.
9	An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications Over Mobile Ad-Hoc Networks[9]	C. Chou, D. Wei, C. Kuo, and K. Naik	Efficient anonymous communication protocol	Less packet loss.	Does not applicable for large-scale networks.
10	Identity-Based Secure Collaboration in Wireless Ad Hoc Networks[10]	J. Pan, L. Cai, X. Shen, and J. Mark	Identity-based cryptography	High remaining energy.	Does not focus on the competitive pricing of selfish peers

11	Efficient Time Synchronization Mechanism for Wireless Multi Hop Networks[11]	B. Wehbi, A. Laouiti, and A. Cavalli	Efficient Time Synchronization Mechanism.	High synchronization precision is achieved.	Effect of mobility and the change of the reference node on the synchronization is not considered.
12	DSC:Cooperation incentive mechanism for multi-hop cellular networks[12]	M. Mahmoud and X. Shen	Cooperation Incentive Mechanism.	High packet delivery ratio.	High complex.
13	Pi: A Practical Incentive Protocol for Delay Tolerant Networks[13]	R. Lu, X. Lin, H. Zhu, X. Shen, and B.R. Preiss	Practical incentive (Pi) protocol.	High delivery ratio and lower average delay.	Integrate Pi with anonymity is not addressed.
14	ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-Hop Wireless Networks[14]	M. Mahmoud and X. Shen	Secure cooperation incentive protocol	Average packet overhead is less.	Highly complex.
15	An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Drop in Multihop Wireless Networks[15]	M. Mahmoud and X. Shen	TRIPO Mechanism.	Improve the network performance in terms of packet delivery ratio.	Integrate the nodes' past behavior into routing decisions is not considered.
16	FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Hybrid Ad Hoc Networks[16]	Mahmoud and X. Shen	Fair and efficient incentive mechanism	Reduce the overhead.	Less detection accuracy.

III. CONCLUSION

This survey presents several payment schemes for improving security with less computation overhead in multi-hop wireless networks. Receipt based method is one of the methods in which the accounting center accumulates and organizes the credit account of the nodes. But in the receipt based scheme has more overhead. In the tamper-proof-device (TPD)-based payment scheme, a tamper-proof-device is installed in every node and organize the credit account for securing the operation. But the drawback is nodes cannot communicate if they do not have adequate credits during the communication time. Regrettably, the nodes at the network border cannot earn as many credits as the other nodes because they are less recurrently preferred by the routing protocol. At the end of this survey conclude that effective method is proposed to improve the security with less processing overhead and complexity in multi-hop wireless networks.

REFERENCES

[1] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Aug. 2000.

[2] S. Zhong, J. Chen, and R. Yang, "Sprite: A Simple, Cheat-Proof, Credit Based System for Mobile Ad-Hoc Networks," In Proceedings of 22nd Annual Joint Conference of the IEEE Computer and Communications, from Mar. 30 to Apr. 3, 2003.

[3] Luzi Aderberg,Stephen Eidenbenz,"A Truthful and cost-efficient routing protocol for mobile adhoc network with selfish agents", In Proceedings of the 9th Annual International Conference on Mobile Computing and Networking, New York, USA, Sep. 2003.

[4] Yanchao Zhang, Wenjing Lou, Yuguang Fang, "SIP: A Secure Incentive Protocol against Selfishness in Mobile Ad Hoc Networks," In proceedings of Wireless Communications and Networking Conference, Mar. 2004.

[5] L. Buttyan and J. Hubaux, "Stimulating Cooperation in Self- Organizing Mobile Ad Hoc Networks," Mobile Networks and Applications, ISSN: 1572-8153, vol. 8, no. 5, Oct. 2004, pp. 579-592.

[6] K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "Authenticated Routing for Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, ISSN: 0733-8716, vol. 23, no. 3, Mar. 2005, pp. 598- 610.

[7] A. Weyland, "Cooperation and Accounting in Multi-Hop Cellular Networks," PhD thesis, Univ. of Bern, Nov. 2005.
[8] G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, "Cooperation Enforcement Schemes for MANETs: A Survey," Wireless Communications and Mobile Computing, vol. 6, no. 3, May. 2006, pp. 319-332.
[9] C. Chou, D. Wei, C. Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications Over Mobile Ad-Hoc Networks," IEEE Journal on Selected Areas in Communications, ISSN: 0733-8716, vol. 25, no. 1, Jan. 2007, pp. 192-203.
[10] J. Pan, L. Cai, X. Shen, and J. Mark, "Identity-Based Secure Collaboration in Wireless Ad Hoc Networks," International Journal of Computer and Telecommunications Networking, ISSN: 1389-1286, vol. 51, no. 3, Feb. 2007, pp. 853-865.
[11] B. Wehbi, A. Laouiti, and A. Cavalli, "Efficient Time Synchronization Mechanism for Wireless Multi Hop Networks," In Proceedings of IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications(PIMRC), Cannes, Sep. 2008.
[12] M. Mahmoud and X. Shen, "DSC: Cooperation incentive mechanism for multi-hop cellular networks," In Proceedings of IEEE International conference on communications, Dresden, from Jun. 14 to Jun. 18, 2009.
[13] 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, ISSN: 1536-1276, vol. 9, no. 4, Apr. 2010, pp. 1483-1493.
[14] M. Mahmoud and X. Shen, "ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-Hop Wireless Networks," IEEE Trans. Mobile Computing, vol. 10, no. 7, July 2011, pp. 997- 1010.
[15] M. Mahmoud and X. Shen, "An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Drop in Multihop Wireless Networks," IEEE Transactions on Vehicular Technology, ISSN: 0018-9545, vol. 60, no. 8, Oct. 2011, pp. 3947-3962.
[16] M. Mahmoud and X. Shen, "FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Hybrid Ad Hoc Networks," IEEE Transactions on Mobile Computing, ISSN: 1536-1233, vol. 11, no. 5, May 2012, pp. 753-766.

