AN ENERGY EFFICIENT ACKNOWLEDGEMENT-BASED METHOD FOR SELFISH NODE DETECTION AND AVOIDANCE IN OPEN MANET

MEHRNAZ NIKMARAM

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JULY 2014

This thesis is dedicated to my beloved parents for their endless support and encouragement.

ACKNOWLEDGMENTS

First and foremost, I would like to sincerely thank my lovely parents, Mahmoud Nikmaram and Mahnaz Parsa, my lovely brother Mohammad Ali , my lovely sisters Behnaz and Farahnaz and all friends for their endless love, support and encouragement. I could not have done it without you! There is no word I can find to thank you.

Then I would like to express my sincere gratitude to my supervisor **Dr. Hassan Chizari** for his continued support during this project. They inspired me greatly to work in this project. Their willingness to motivate me contributed tremendously to the success of this project. I have learned a lot from them and I could not have imagined having a better advisor and mentor for my Master study. Many thanks to all my lecturers, I will forever be grateful.

Besides, I would like to thank my examiners: **Dr. Anazida Binti Zainal, Dr. Kamalrulnizam Bin Abu Bakar, Dr.Maznah Binti Kamat, Dr. Majid Bakhtiari and Dr. Maheyzah MD. Siraj,** for their patience and insightful comments.

Finally, I would like to thank Universiti Teknologi Malaysia for their kind cooperation.

ABSTRACT

Mobile Ad-Hoc Networks (MANET) is a decentralized infrastructure with relatively low capacity of connections for communication with the special measures described as a collection of autonomous mobile nodes. In such networks, weak communication links and node mobility can lead to highly unpredictable and dynamically changing topologies. Open MANET is one of the types of MANET in which any node is able to join or leave the network. Thus, it is vulnerable in oppose of selfish nodes which they do not like to spend their resources to participate in network activities such as routing. This helps them to preserve their limited energy while they have a huge negative impact on the network performance and total energy usage. One of the category of methods to for selfish node detection and avoidance is acknowledgement-based methods. Negative Acknowledgement (NACK) is the best method for detecting and avoidance selfish node in this category. The NACK method has high level of packet delivery, and high throughput in opposed of misbehaving action. However, this method suffers from extra charge by number of routing overhead, and more energy consumption when number of selfish nodes or mobility of nodes are increasing. In this study, using the Selective Acknowledgement (SACK) a new selfish node detection method has been developed called S-NACK. This method uses SACK instead of full TCP over the NACK. The proposed method was implemented in NS2 and its performance was compared with NACK. The extensive simulation results showed that S-NACK reduces the network overhead and improves the energy consumption in comparison to NACK whereas the packet delivery ratio is almost similar at the same time.

ABSTRAK

Mobile Ad-Hoc Networks (MANET) adalah infrastruktur berpusat dengan kapasiti sambungan komunikasi yang rendah dengan langkah-langkah khas digambarkan sebagai koleksi nod yang bergerak sendiri. Dalam rangkaian-rangkaian tersebut, hubungan komunikasi dan mobiliti nod yang lemah boleh mengakibatkan topologi yang sangat tidak menentu dan berubah secara dinamik. MANET terbuka adalah salah satu jenis MANET di mana mana-mana nod mampu untuk menyertai atau meninggalkan rangkaian. Oleh itu, ia terdedah dalam menentang nod yang menyendiri dimana sumber-sumber tidak mudah dihabiskan semasa mengambil bahagian dalam aktiviti-aktiviti rangkaian seperti penghalaan. Hal ini amat membantu dalam mengekalkan tenaga yang terhad semasa memberi kesan negatif yang besar kepada prestasi rangkaian dan jumlah penggunaan tenaga. Salah satu kaedah untuk mengesan nod ini dan bagi mengelakkannya adalah kaedah perakuan berasas. Negative Acknowledgement (NACK) adalah kaedah yang terbaik bagi mengesan dan mengelakkan nod yang menyendiri dalam kategori ini. kaedah NACK mempunyai tahap penghantaran paket, dan pemprosesan yang tinggi dalam penentangan daripada menimbulkan tindakan negatif. Walau bagaimanapun, kaedah ini mengalami caj tambahan dengan beberapa laluan beban dan penggunaan tenaga yang lebih apabila bilangan nod yang menyendiri atau mobiliti nod semakin meningkat. Dalam kajian ini, dengan menggunakan Selective Acknowledgement (SACK), kaedah pengesanan nod baru yang menyendiri telah dibangunkan dam dipanggil sebagai S-NACK. kaedah ini menggunakan SACK dan bukannya TCP penuh ke atas NACK. kaedah yang dicadangkan telah dilaksanakan pada NS2 dan prestasinya telah dibandingkan dengan NACK. Keputusan simulasi yang luas menunjukkan bahawa S-NACK mengurangkan beban rangkaian dan meningkatkan penggunaan tenaga berbanding NACK, manakala nisbah penghantaran paket adalah hampir sama pada masa yang sama.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Mobile Ad Hoc Network (MANET) is composed of a number of autonomous, self-organize, resource constraint, and mobile nodes, which communicate with each other over, low capacity links. These networks suffer from lack of centralized infrastructure. The network topology in MANET is dynamic because of mobility of nodes. Therefore, the MANET suffers from dynamic and unpredictable links. Each node performs the network functions in MANET individually or collaboratively with other nodes. For example, the routing is done in collaboration with other nodes. The collaborative functions that need to collaboration of a set of nodes in network have a direct impact in network performance. MANET is employed in different military and civilian applications such as healthcare, monitoring, and so on.

In general, based on the user of MANET, it can be divided into two types including (Miranda and Rodrigues, 2002). In open MANET, there are different users with various aims; these users collaborate with each other with sharing their resources in order to gain connectivity to other nodes which are not in their communication range. In contrast, closed MANET is composed of a number of nodes with common authority controls. The nodes in close MANET act collaboratively with each other to achieve the same goal. Due to characteristics of open MANET, they are prone to appearance of misbehaving nodes such as selfish nodes. Selfish nodes can exist in the network because

of couple of reasons. First, since the communication medium is open in open MANET, mobile hosts suffer from lack of suitable physical protection, which makes vulnerable these networks to misbehavior actions. Second, most of the mobile hosts suffer from resource-constraint and performing the collaborative network functions needs to considerable amount of resource wasting such as energy, memory, and so on. Hence, some of nodes (i.e., selfish nodes) consciously don't participate in collaborative functions in order to save their limited resource. Since the MANET suffers from lack of centralized management system, detecting this selfish nodes and prevention of the misbehaviour actions is a so challenging problem in these networks.

The misbehaviour by selfish node is different from malicious behaviour. In fact, the selfish nodes use the network for own goals and they don't participate in collaborative tasks for helping to other nodes to save their own limited resources. However, their aim is not to damage the network. In contrast, the mission of malicious nodes is wasting the limited resource of other nodes to damage the network.

The Transmission Control Protocol (TCP) is one of main protocols in transport layer in protocol stack. This mission of this protocol is providing a reliable end-to-end data transmission. Due to memory constraints, packet loss is one of major problems with using TCP over MANET. While the mobile ad hoc networks suffer from losses due to errors or mobility and links. In addition, different reactions are needed for packet losses.

TCP New Reno introduced by Allman et al. (2001), to avoid timeouts in the case of multiple segments lost from the same window by staying in the fast retransmit/fast recovery phase until all the segments are correctly received. The packet losses, which are made use to a window of data, have a dramatic impact on throughput of TCP. TCP employ a cumulative acknowledgment method. In this method, the received segments which are not at the left edge of the receive window, and are not acknowledged. This situation forces the sender node to find out each lost packet and unnecessarily retransmits a correctly received segment or wait a round-trip time. Cumulative acknowledgment method suffers from multiple dropped segments. Therefore, the TCP

loses its ACK-based clock and overall throughput is reduced. To handle this problem, Selective Acknowledgment (SACK) is proposed. Using the selective acknowledgments, all successful received segments are informed to sender. Consequently, the sender needs to only retransmit those segments that actually have been lost. TCP SACK recuperates all segments lost from the current window faster than TCP New Reno by having specific information about the packets in flight and the ones correctly received (Fall, K. and S. Floyd 1996).

1.2 Problem background

Owing to MANET characteristics there are variety kinds of challenges in Ad-hoc networks such, as the nodes in MANET are energy constrained because they supply by battery. Also, open MANETs are vulnerable to selfish nodes so that the selfish nodes perform misbehaviour actions and significantly decrease the packet delivery rate. Third, transport layer such as TCP in MANET is not efficient due to several reasons specific to these networks: loss channels, path asymmetry, network partitions, route failures, and power constraints. Fourth, the MANET suffers from dynamic network topology, which handling the mobility make more overhead in different functions such as communication protocols.

According to MANET characteristics, packet dropping by selfish nodes is an abnormal action, which can drop the network performance. To deal with this problem, the selfish nodes should be detected and avoided to improve the network performance.

Hop-by-hop detection and end-to-end detection are two main approaches for detecting the selfish nodes in open MANET in order to avoid the abnormal actions and improve the packet loss. End-to-End detection methods are focused on packet mission time and forwarder will be forward incoming packet until destination. Detection and analysis are occurred on destination. In contrast, Hop-by-hop detection methods are focused on message authentication and every intermediate or forwarder can detect the

messages originality whether or not the messages come from the trusted nodes, sent to next hop or dropped by next/last hop. En-route filtering methods are well-known candidate in this category. Also, Hop-by-hop detection can be successful when it is associated with routing acknowledgement.

In MANET it is assume that all nodes cooperative work with each other in trustworthy way. Therefore, the routing and delivering a packet from source to destination is possible. However, some of nodes cannot take part in network activities due to resource limitations such as low battery. According to Buttyan and Hubaux (2008), a node that only use the other nodes resources for own benefit and doesn't help to other nodes in network activities called selfish node. If a selfish node exists in a route, routing in this route lead to packet loss and this route is called misbehaviour route. To handle the misbehaviour route, the source nodes discover the new route. However, this route may compose of a selfish node. Therefore, due to misbehaviour routes, the packet delivery ratio is reduced significantly. To detect and reduce the impact of misbehaviour routes in MANETs, several methods have been introduced in literatures. Some of the techniques use a credit-based method (Buttyan and Hubaux, 2003; Zhong *et al*., 2003; Wang and Li, 2006; Eidenbenz *et al*., 2008). The key problem of credit-based method is that these methods usually need to a hardware called tamper-resistant to protect the virtual currency or an extra payment system. The second group is techniques use a reputation-based method (Marti *et al*., 2000; Buchegger and Boudec, 2002; Liu and Yang, 2003). Marti et al. (2000) introduced two models for detecting the selfish node called watchdog and path rater. The watchdog use overhearing to detect the selfish nodes whereas, the path rater avoid the selfish nodes in route discover procedure. The overhearing method is not efficient to detecting the selfish nodes in MANET because the transmission is unstable in MANET to handle this problem; Liu *et al.* (2007) introduced an acknowledgment-based approach to overcome the weaknesses of overhearing. They propose two-hop acknowledge packets as receipts method (2ACK) in order to a node can confirm whether or not its next-hop forwards the data packets.

Negative Acknowledgment (NACK) is defined as an acknowledgment-based approach method that is focused on negative acknowledgment. NACK proposed by Jeba

and Paramasivan (2012) to prevent routing abnormal action. This method can detect misbehaviour actions based on reply ACK to last two nodes in MANET chain. In this method, each node will monitor by last two nodes. Figure 1.2 shows the quick method of NACK communications between S as the source and D as the Destination and N_i as the intermediate node. Although NACK can detect most of abnormal actions in communication chain, via applying this method, network availability will be endangered. Sending reply packet to two last nodes for all incoming packets generate high overhead and needs much power and great bandwidth. Due to the characteristics of nodes, they are suffering from low power computing and low bandwidth (Jeba and Paramasivan , 2012).

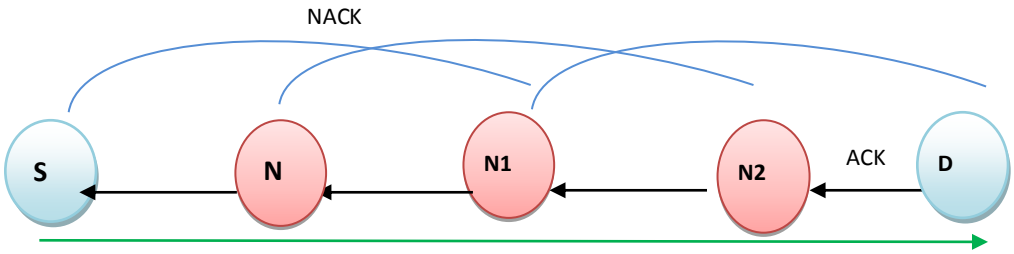

Figure 1.1 NACK method (Sun *et al.*, 2012)

Considerable factors to network availability assessment are presented as communication protocol. NACK improves the packet delivery rate in communication protocols with detecting and avoiding the selfish nodes. However, the negative feedback of NACK can be justified by its high overhead and high-energy consumption in communication Protocol. Regards to NACK nature, this method is constructed based on duplex TCP connection. Therefore, a novel solution should be designed and developed to utilize the NACK advantages, while focus on reducing the network overhead and energy consumption.

1.3 Problem Statement

Selfish nodes in open MANET generate an abnormal behaviour. For example, in communication protocols if a selfish node is selected as a node in the path from source to destination; it will not participate in routing process to save its constraint resources. Therefore, the routing process is failed and undergoes a high overhead to discover another path from source to destination node, which may contain another selfish node in between, cause's packet loss and a drop in the packet delivery rate. Consequently, the network performance will be significantly reduced. Detection of misbehaviour or selfish nodes in network and avoiding these nodes to prevent the abnormal actions in the routing process is one of the most important problems in open MANET. Acknowledgement based selfish node detection and avoidance approaches is most promising method to this end. Among the existing acknowledgement based approaches, the Negative Acknowledgement (NACK) method has suitable selfish node detection and avoidance results. However, the method, which is designed for this end, suffers from high overhead, which leads to high-energy consumption. Since the energy of a node is supplied by battery and the changing and replacing of the battery is too costly in MANET, enhancing the existing NACK method by low overhead mechanisms which leads to reduction in network overhead and improve the energy consumption is essential due to energy constraints node in MANET.

1.4 Purpose of the Study

The main goal of this research is to design and develop an energy efficient acknowledgement based misbehaviour node detection and avoidance method for open MANET with selfish nodes to mitigate the communication overhead and improves the energy consumption while preserving the packet delivery rate.

1.5 Research Questions

Based on the purpose and requirements of the study, the general research question is: How to design an energy efficient acknowledgement-based misbehaver node detection and avoidance method in open MANET with low overhead and good packet delivery rate?

In order to be able to answer this question, a set of research questions is presented as follows:

i. How to mitigate the overhead of different acknowledgements messages to reduce the network overhead?
ii. How to decrease the energy consumption to improve the packet delivery rate?
iii. How NACK can improved based on energy and overhead?

1.6 Objective of the Study

To attain research aim, the following research objectives have been identified:

i. To investigate current acknowledgement based misbehavior node detection method and formulating the problem.
ii. To design and develop an energy efficient acknowledgement based misbehaver node detection and avoidance method for open MANET.
iii. To evaluate and validate the performance of the proposed method.

1.7 Significance of the Study

Misbehaviour node detection and avoidance problem in MANET is a challenging problem in which usually the network performance is scarified to improve the detection rate. As in MANET nodes have limited resource of energy, finding a method, which can preserve the detection rate of misbehaviour nodes while improving the network performance metrics such as energy consumption is an important issue. This research introduces a solution to acknowledgement based misbehaviour node detection and avoidance problem in open MANET. This proposed method improves the network overhead and network energy consumption of mobile nodes while the packet delivery is almost similar to existing methods.

1.8 Scope of the Study

The scope of this study is limited to some key points as follow:

i. This research mainly focuses on acknowledgement-based detection and avoidance of selfish nodes problem in open MANET and, at the same time, improve the network overhead and energy consumption.
ii. All normal and selfish nodes are randomly and uniformly scattered in a two dimensional area.
iii. The implementation of previous and proposed methods based on DSR routing protocol.

1.9 Organization of the Study

This thesis is organized into six chapters. Chapter 1 introduces the overall plan of this research. Chapter 2 reviews the literature related to misbehaviour nodes

detections and avoidance methods and overhead suppressing and energy improvement in MANET following by Chapter 3 to present the research methodology that is conducted in this research. Chapter 4 introduces acknowledgement based misbehaver node detection and avoidance problem and proposes an energy efficient method for solving this problem. In Chapter 5, the finding and discussion presented. Finally, Chapter 6 concludes the thesis and presents the limitations and contributions of the present research.

REFERENCES

Aarti, D. S. 2013. "Tyagi," Study of MANET: Characteristics, Challenges, Application and Security Attacks,"." International Journal of Advanced Research in Computer Science and Software Engineering 3(5): 252-257.

Ahmed, M. R., X. Huang, et al. 2012. "A Taxonomy of Internal Attacks in Wireless Sensor Network." Memory (Kbytes) 128: 48.

Akyildiz, I. F., W. Su, et al. 2002. "A survey on sensor networks." Communications magazine, IEEE 40(8): 102-114.

Al Hanbali, A., Altman, E., & Nain, P. 2005. A survey of TCP over ad hoc networks. *IEEE Communications Surveys and Tutorials, 7*(1-4), 22-36.

Allman, M., Balakrishnan, H., & Floyd, S. 2001. *Enhancing TCP's loss recovery using limited transmit*. RFc 3042, January.

Balakrishnan, K., J. Deng, et al. 2005. TWOACK: preventing selfishness in mobile ad hoc networks. Wireless Communications and Networking Conference, 2005 IEEE, IEEE.

Chiang, M. 2005. Balancing transport and physical layers in wireless multihop networks: Jointly optimal congestion control and power control. *Selected Areas in Communications, IEEE Journal on, 23*(1), 104-116.

Corson, M. S., J. P. Macker, et al. 1999. "Internet-based mobile ad hoc networking." Internet Computing, IEEE3(4): 63-70.

Ertaul, L. and N. Chavan 2005. Security of ad hoc networks and threshold cryptography. Wireless Networks, Communications and Mobile Computing, 2005 International Conference on, IEEE.

Eschenauer, L. and V. D. Gligor 2002. A key-management for distributed sensor networks. Proceedings of the 9th ACM conference on Computer and communications security, ACM.

Fall, K. and S. Floyd 1996. "Simulation-based comparisons of Tahoe, Reno and SACK TCP." ACM SIGCOMM Computer Communication Review26(3): 5-21.

Fecko, M. A., U. C. Kozat, et al. 2004. Architecture and applications of dynamic survivable resource pooling in battlefield networks. Defense and Security, International Society for Optics and Photonics.

Goyal, P., V. Parmar, et al. 2011. "Manet: vulnerabilities, challenges, attacks, application." IJCEM International Journal of Computational Engineering & Management 11: 32-37.

Hou, H., C. Corbett, et al. 2007. Dynamic energy-based encoding and filtering in sensor networks. Military Communications Conference, 2007. MILCOM 2007. IEEE, IEEE.

Hu, Y.-C., A. Perrig, et al. 2006. "Wormhole attacks in wireless networks." Selected Areas in Communications, IEEE Journal on 24(2): 370-380.

Ilyas, M. 2002. The handbook of ad hoc wireless networks, CRC press.

Issariyakul, T. 2012. Introduction to network simulator NS2, Springer Science+ Business Media.

Jacobson, V. and R. Braden "RFC 1072: TCP extensions for long-delay paths, October 1, 1988." Obsoleted by RFC1323 [11].

Jeba, S. A. and B. Paramasivan 2012. "False Data Injection Attack and its Countermeasures in Wireless Sensor Networks." European Journal of Scientific Research 82(2): 248-257.

Jones, C. E., Sivalingam, K. M., Agrawal, P., & Chen, J. C. 2001. A survey of energy efficient network protocols for wireless networks. *wireless networks*, *7*(4), 343-358.

Karlof, C. and D. Wagner 2003. "Secure routing in wireless sensor networks: Attacks and countermeasures." Ad Hoc Networks 1(2): 293-315.

Kang, N., Shakshuki, E. M., & Sheltami, T. R. 2010. Detecting misbehaving nodes in MANETs. In *Proceedings of the 12th International Conference on Information Integration and Web-based Applications & Services* (pp. 216-222). ACM.

Klemm, F., Krishnamurthy, S. V., & Tripathi, S. K. 2003. Alleviating effects of mobility on tcp performance in ad hoc networks using signal strength based link management. Paper presented at the Personal Wireless Communications.

Kraub, C., M. Schneider, et al. 2007. STEF: A secure ticket-based en-route filtering scheme for wireless sensor networks. Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on, IEEE.

Lamport, L., R. Shostak, et al. 1982. "The Byzantine generals problem." ACM Transactions on Programming Languages and Systems (TOPLAS)4(3): 382-401.

Lavanya.K 2014. "Detecting Forged Acknowledgement in Mobile Ad-Hoc Network Using Intrusion Detection System." International Journal of Innovative Research in Computer and Communication Engineering 2(1): 7.

Logeshwari, C., & Priya, N. G. 2010. A Survey on Secure Intrusion Detection for Detecting Malicious Attackers in MANETs.

Liu, K., J. Deng, et al. 2007. "An acknowledgment-based approach for the detection of routing misbehavior in MANETs." Mobile Computing, IEEE Transactions on 6(5): 536-550.

Lu, R., X. Lin, et al. 2012. "Becan: A bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks." Parallel and Distributed Systems, IEEE Transactions on23(1): 32-43.

Marti, S., Giuli, T. J., Lai, K., & Baker, M. 2000. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking (pp. 255-265). ACM.

Mathis, M., J. Mahdavi, et al. 2000. RFC 2883: An Extension to the Selective Acknowlegdment (SACK) Option for TCP, July.

Mathis, M., J. Mahdavi, et al. 1996. RFC 2018: TCP selective acknowledgment options, October.

Mohanty, P., S. Panigrahi, et al. 2010. "SECURITY ISSUES IN WIRELESS SENSOR NETWORK DATA GATHERING PROTOCOLS: A SURVEY." Journal of Theoretical & Applied Information Technology13.

Parker, J. Discussion Record for the 1st MANET Reading Group Meeting.

Ramarathinam, V. and M. A. Labrador 2002. Performance analysis of TCP over static ad hoc wireless networks. Proceedings of the ISCA 15th International Conference on Parallel and Distributed Computing Systems (PDCS), Citeseer.

Rao, P. S. S., A. Meher, et al. "Detection of Routing Misbehavior Nodes Using Improved 2-ACK in MANET'S (Simulation through NS-2)."

Sharma, K. and M. Ghose 2010. "Wireless sensor networks: An overview on its security threats." IJCA, Special Issue on “Mobile Ad-hoc Networks” MANETs.

Singh, P. K. and G. Sharma 2012. An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET. Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on.

Stevens, W. R. 1997. TCP slow start, congestion avoidance, fast retransmit, and fast recovery algorithms.

Sun, B., L. Osborne, et al. 2007. "Intrusion detection techniques in mobile ad hoc and wireless sensor networks." Wireless Communications, IEEE 14(5): 56-63.

Sun, H.-M., C.-H. Chen, et al. 2012. "A novel acknowledgment-based approach against collude attacks in MANET." Expert Systems with Applications 39(9): 7968-7975.

Taneja, S., & Kush, A. 2010. A Survey of routing protocols in mobile ad hoc networks. *International Journal of Innovation, Management and Technology*, *1*(3), 2010-0248.

Tuexen, M., Q. Xie, et al. 2002. Architecture for reliable server pooling. Mobile Computing and Communications Review, January, Citeseer.

Uluagac, A. S., R. A. Beyah, et al. 2010. "VEBEK: Virtual energy-based encryption and keying for wireless sensor networks." Mobile Computing, IEEE Transactions on 9(7): 994-1007.

Weisser, M. 1991. "The computer for the twenty-first century." Scientific American 265: 94-104.

Xinyu, Y., L. Jie, et al. 2012. A Novel En-route Filtering Scheme against False Data Injection Attacks in Cyber-Physical Networked Systems. Distributed Computing Systems (ICDCS), 2012 IEEE 32nd International Conference on.

Yang, H. and S. Lu 2004. Commutative cipher based en-route filtering in wireless sensor networks. Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th, IEEE.

Ye, F., H. Luo, et al. 2005. "Statistical en-route filtering of injected false data in sensor networks." Selected Areas in Communications, IEEE Journal on 23(4): 839-850.

Yu, Z. and Y. Guan 2010. "A dynamic en-route filtering scheme for data reporting in wireless sensor networks." IEEE/ACM Transactions on Networking (ToN) 18(1): 150-163.

Zhang, Y., W. Liu, et al. 2006. "Location-based compromise-tolerant security mechanisms for wireless sensor networks." Selected Areas in Communications, IEEE Journal on 24(2): 247-260.

Zhou, Y., Y. Fang, et al. 2008. "Securing wireless sensor networks: a survey." Communications Surveys & Tutorials, IEEE 10(3): 6-28.

Zhu, S., S. Setia, et al. 2004. An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks. Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on, IEEE.