FALSE DATA DETECTION IN MOBILE AD-HOC NETWORK BASED ON DIGITAL SIGNATURE

BABAK EMAMI ABARGHOUEI

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

Faculty of Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2013

I dedicated this thesis to my beloved Mother For her endless support and encouragement

ACKNOWLEDGEMENT

IN THE NAME OF GOD, MOST GRACIOUS, MOST COMPASSIONATE

I would like to acknowledge my supervisor, **Dr.ISMAIL FAUZI BIN ISNIN**, for his support, encouragement, guidance, astute and expert editing. I would like to express gratitude for his patience, generosity, and collaboration.

My lovely family; thank you for your perpetual encouragement and support. Your unwavering love that have shaped my mind and opened the doors of opportunity leading me to become the person I am today.

I would like to thank all of the individuals who have helped me during my thesis study.

ABSTRACT

Routing misbehavior and false communication on wireless sensor network are so significant. An attacker can devour the sensor resources. No central monitoring system, lead to mobile sensor network suffering false communication. This thesis, organized to introduce a new detection method to mitigate the effect of false data on the mobile AD-HOC network. DNACK, which proposed in this thesis, Is a new modification of NACK method. DNACK also consider about negative acknowledgment to find the false route messages. DNACK can detect modified messages in the middle of a route in oppose of NACK which, can detect false modified data on the destination. By comparison, the Delivery percentage on NACK and DNACK, DNACK shown better results in opposed to NACK method. Simulation has been done in three modes of node's mobility Speed in meter per second (M:0 , M:5 and M; 10). In all situations, the efficiency of DNACK is better than NACK because in NACK nodes all packets (original and modified) are delivering to destination by contrast in DNACK just original packets are deliver to destination. However the Delivery percentage in NACK is Higher than DNACK which is around 2% for 10 meters per second nodes' movement .Nevertheless DNACK is more efficient than NACK .On M=10 (m/s) DNACK shown 64% verified messages on Destination in opposed by 60% verified messages on NACK method. In overall the efficiency of packet delivery can be calculated by multiplication of overall delivery by verified packet shows that DNACK method has 51.5 % verified messages delivery in opposed of NACK by 49.8 % delivery on M=10 m/s.

ABSTRAK

Salah laku routing dan komunikasi palsu pada rangkaian pengesan tanpa wayar amat ketara. Penyerang boleh mengambil sumber-sumber pengesan tersebut. Ketiadaan pusat sistem pemantauan, boleh membawa kepada rangkaian pengesan mudah-alih mengalami komunikasi palsu. Kajian ini dijalankan untuk memperkenalkan suatu kaedah pengesanan yang baru untuk mengurangkan kesan data palsu pada rangkaian mudah-alih AD-HOC. DNACK, yang dicadangkan dalam kajian ini, adalah pengubahsuaian baru pada kaedah NACK. DNACK juga mempertimbangkan tentang pengakuan negatif untuk mencari laluan mesej-mesej palsu. DNACK boleh mengesan mesej-mesej yang telah diubahsuai semasa ia dalam laluan, manakala NACK boleh mengesan data yang telah diubahsuai pada destinasi. Secara perbandingan, peratus penghantaran pada NACK dan DNACK, DNACK menunjukkan keputusan yang lebih baik berbanding dengan kaedah NACK. Simulasi telah dijalankan pada 3 mod pergerakan kelajuan nod-nod dalam meter sesaat (M:0 , M:5 and M; 10). Dalam semua situasi, keberkesanan DNACK adalah lebih baik dari NACK kerana dalam NACK kesemua paket-pakes nod (yang asal dan diubahsuai) dihantar kepada destinasi sementara DNACK hanya menghantar paket-paket yang asli kepada destinasi. Walau bagaimanapun, peratus penghantaran NACK adalah lebih tinggi daripada DNACK iaitu dalam sekitar 2% untuk 10 meter sesaat pergerakan nod-nod. Namun DNACK mempunyai kecekapan yang lebih baik dari NACK. Pada M=10 (m/s) DNACK memperolehi 64% mesej-mesej yang disahkan pada destinasi manakala hanya 60% mesej-mesej yang disahkan dengan menggunakan kaedah NACK. Secara keseluruhanya, kecekapan penghantaran paket boleh dikira dengan membuat pendaraban keseluruhan penghantaran oleh paket yang disahkan menunjukkan bahawa kaedah DNACK mempunyai peratus penghantaran mesej-mesej yang disahkan 51.5% manakala NACK mempunyai 49.8% penghantaran pada M=10 m/s.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURE

CHAPTER 1

INTRODUCTION

1 .1 Introduction

MANET or Mobile AD-HOC Network is a wireless system that embraces mobile nodes. It is generally denoted to a decentralized autonomous system. MANET does not require any fixed infrastructure such as base stations, router, infrastructure, and therefore, it is an attractive networking option for connecting mobile devices quickly and spontaneously to environments such as military battlefields and rescue operations.

Mobile nodes consist of mobile devices as well as mobile phone, laptop, home computer, MP3 player, PDA or personal digital assistant. Mobile Nodes can be applied in a variety of gadgets, such as ships, airplanes, or land, irrespective of their location as they can participate in communication. Decentralized autonomous feature leads to MANET to have some special feature such as self-connectivity and easy deployment. These features of MANETs make it the best candidate in challenging situations such as emergency, surveillance and rescue operations.

However those characteristic make MANET as so interesting object of communication but also having no central monitoring system , fixed infrastructure and nodes self-configuration lead to confidential or secure communication on Mobile nodes faced by high cost.

GCSs or secure group communication systems required a confident secure architecture. Due to special characteristic MANET Security faced by some technical challenges such as “resource-constrained environments (e.g., Bandwidth, memory size, battery life, and computational power), openness to eavesdropping and security threats, unreliable communication, no infrastructure support, and rapid changes in network topology due to user mobility which could cause group merge/partition events to occur dynamically”(Cho and Chen 2011). MANET Nodes’ mobility is the most specific characteristic in whole AD-HOC Network domain.

1.1.1 MANET Characteristics

A. **Dynamic network topology:** because of nodes’ mobility, network structure modified constantly. Network domain may have different cluster or zone , according to nodes’ motivation , a node might be left its zone and joined to another zone or even joined to one another network .
B. **Energy constrained nodes:** due to nodes’ mobility, MANET need to have embedded low power instead of direct power, Manet’s nodes will most often rely on batteries as their power source. Because of this limitation AD-HOC nodes cannot support the heavy computing algorithm
C. **Bandwidth’s restriction:** low power nodes and low power computing leads to Mobile nodes face by some limitation on bandwidth. This may effect on the number and messages’ size during communication.
D. **Lack of physical security:** fading the central physical monitoring system because of Nodes’ motion ability leads to exposure of the network nodes increase the possibility of attacks against the network. Owing to nodes’ mobility, the risk of physically compromised/ tampering by ID spoofing and so forth is bigger than outmoded network nodes.

1.2 Background of the Study

Considering to MANET characteristic, vast of majority researches have been proposed to solve MANET security challenge such as routing protocols, secure routing protocols, trusted base party and so forth. Dynamic routing protocol limitation has been covered by different routing protocol, can be introduced into a majority of routing link-state and distance vector.

1.2.1 MANET Routing Protocol

MANET gradually exploited the wireless communication world as the common means of human communication. Devices are configured with Wi-Fi cards as hotspots in many places such as universities, offices, airports, and hotels. It stood as a major source of communication in this modern world. This challenged the researchers around the world to enforce their research in developing MANET. In such advanced communication network, routing protocol plays a key role, as it is one of the major aspects to route the data in a network. Many researchers have proposed different protocols.

MANET routing protocol noticed experimental Request For Comments (RFC) since 2003.Implementation and deployment of the protocols have not properly addressed by RFCs, but the routing protocol algorithms proposed were identified as trial technology with the high probability that will result into a standard. Enormous research work has been focused on different routing protocols such as Dynamic Source Routing (DSR), Optimized Link State routing(OLSR), Temporarily Ordered Routing Algorithm (TORA) and Ad hoc On-demand Distance Vector (AODV), for their development and standardization of routing support from MANET Working group(WG) of Internet Engineering Task Force (IETF) (Luo, Ye et al. 2009). The aim of proposing the variety of routing protocols in different shape there was nothing else to except approaching the high level of network security.

Secure mobile network necessities like privacy, authentication, integrity and non-repudiation rely on a secure key management framework.(Bala Krishna and Doja 2011)

1.2.2 MANET Security Goal

A. **Confidentiality** makes sure that the transmitted data packet is not being exposed to unauthorized users.
B. **Availability** makes sure that the resource will be available to trusted party and unavailable to unauthorized.
C. **Integrity** confirms that data is not being corrupted or tampered with during transmission. Integrity encompasses data integrity and origin integrity. Data integrity ensures that original content of the data is not altered or tampered with. Origin integrity verifies the sender's identity and ensures that the data has been sent by the appropriate entity.
D. **Authenticity** verifies that a user is permitted or has the proper permission to access or use a resource.
E. **Non-Repudiation** binds a user's identity with his/her action, so that the user cannot deny the action he has performed.

Owing to these goals, communication had to reach the highest level of security that even trusted party cannot understand the communication of its neighborhood. According to networks' confidentiality and integrity, there are vast of majority research have been focused only on misbehavior detection.

In summary, security is a most important part of communication. It cannot be reach to high level of security if even one part of security goal going to neglect. MANET is so interesting to every part of communication as well as the battlefield, medical sensors, body sensor, desert and ocean telecommunication and so forth by considering to C.I.A. The MANET security architecture had to cover each main part, Confidentiality, Integrity and Availability.

1.2.3 Background of Problem

MANET or Mobile AD-HOC network is composed of a an small countable mobile nodes having limited resource such as computation capacity, memory space, low power/computing and low Bandwidth communication. Mobile nodes treated to deployed in hostile environment .In such situation mobile nodes will engaged to variety of attacks for instance false data, masquerade, selective forwarding , eavesdropping and so forth. Attacker can rise up number of attacks from outside as well as inside zone. There are a number of security framework have been proposing to isolate the Mobile nodes in oppose of malicious nodes.

Due to MANET characteristic, there are different kinds of attack in mobile network layers. Table 2.1 contains of some information of common attack on MANET layers. By comparing between those kinds of attacks, false data injection or false communication attack is much more significant. Considering to false data nature, it can cover the variety of routing attacks such as wormhole, false route and modified data. The definition of false data has been discussed in section 2.2.

In a MANET, since all communications are totally exposed and disposed to be captured, an efficient encryption system can be provided the secure communication. Due to MANET limitation such as energy , low power , low power computing , and lack of centralized infrastructure, cryptography method is recommended significantly to prevent of external attack (Bala Krishna and Doja 2011) . But on the other hand crypto system need powerful algorithm and need more power and energy as well , considering to route path and intermediate nodes, misbehavior acting and false data injection detectable by routing table ,much easier than using the crypto system as well as symmetric or Asymmetric methods(Su 2010).

Due to False data attack, there are two basic methods to detect such this kind of attack: en-route filtering and end-to-end detection based on cryptography method. Table 2.2 shown the summarize of false data detection. By comparison, those ideas false data can be controlled by cooperation between these two classes. NACK

method is the en-route monitoring method which, proposed by (Sun, Chen et al. 2012). NACK nodes also are engaged by Digital signature method to detect the modified data in end-to-end path. NACK is significant method which in this thesis tried to simulate this method to detect the false data.

End-to-end detection has been supported by variety researchers considering to MANET limitation, and nature of false data which lets off the attacker to saturate the network Bandwidth. In (CPNS),or Cyber-Physical Networked Systems, unauthorized node could inject false data for controlling through the MANET nodes, which not only threaten on confidentially and integrity of data, but also false data can be lead to consumes the CPU and node power and having action as well as DOS ,or Denial Of Service attack by threatening the network availability(Xinyu, Jie et al. 2012).

Due to mobile nodes limitation, hop-by-hop detection can be much more significant than end-to-end. According to those proposed method for false data detection, by engaging the en-route monitoring method and crypto system together, we can have the much more efficient method for detecting this kind of attack.

Sensor nodes sense the events that occur in their surrounding environment. Generate event report for the sensed information and the event report has to be send to the base station through the en-route nodes. When event report is forwarded through en-route node a compromised node can forge the report. False data contain false information from compromised nodes. This false data injection attack depletes the energy of the en-route nodes. This may be dangerous in scenarios such as battlefield surveillance and environmental monitoring by making false decision. Moreover, it is a difficult task to monitor all the sensor nodes in the field of interest.

However, several recent research efforts have proposed mechanisms to enable node and message authentication in sensor networks, those proposed solutions can prevent false reports injection by outside attackers. They are made ineffective when any single node is compromised. One solution to reduce the impact of false

data injection into the network through a compromised node is to filter the false data by the en-route node as early as possible before reaching the base station. Authentic and accurate data is provided to surrounding sensor node and to the sink through en-route filtering scheme. En-route filtering is an effective way to defeat false data injection attacks .Moreover Messages' authenticity will be check by intermediate nodes as well as destination on en-route filtering methods. Due to this nodes activity the false messages will not be able travelling more and the nodes resources will be survived. This paper describes about many of the existing en-route filtering schemes. In addition analyze about the advantages and disadvantages of the related en-route filtering scheme.

According to previous research in FDD , or False Data Detection , most of them have the same consumption to detect the false data and misbehavior action based on hop-by-hop authentication(Azer, El-Kassas et al. 2008; Su 2010; Abdalla, Saroit et al. 2011; Gupta, Kar et al. 2011).

In (CPNS) or Cyber-Physical Networked Systems, unauthorized node could inject false data for controlling through the MANET nodes, which not only threaten on confidentially and integrity of data, but also false data can be lead to consumes the CPU and node power and having action as well as DOS ,or Denial Of Service attack by threatening the network availability.

A number of en-route filtering methods have been proposing To contract with this issue (Xinyu, Jie et al. 2012). As can be seen there are a number of previous research which focusing on localization nodes in different security methods.

Due significance of the false data, by deep exploration on more than 80 papers on variety method we find NACK(Sun, Chen et al. 2012) method which so interesting method.
NACK member no need to have any extra devices and NACK member can detect false data in the false route so easily. Nevertheless, because of NACK methodology, members can detect the false modified data in end-to-end detection. Due to this

NACK characteristic, we proposed the new method of NACK to improved NACK efficiency while network faced by man in a middle and fabrication messages. DNACK can be detected fabricated message Due to hop-by-hop message authentication.

1.3 Statement of Problem

False communication on wireless sensor network not only absorbed the node's resources also, it can be break down a network such as denial of service attack. The false reports consume lots of network and computation resources and shorten the lifetime of sensor networks. Hence, to ensure the normal operation of the system, it is critical to filter false data at forwarding nodes before arriving at the destination(Jeba and Paramasivan 2012).

Though several recent research efforts have, proposed mechanisms to enable node and message authentication in sensor networks, those proposed solutions mostly considered about false reports or false route messages. In addition, there are countable methods, they are considered about false modified data. According to false data nature, having a security method to detect the false data in false route and modified data by cooperation of intermediate nodes still a challenging problem.

1.4 Purpose of the Study

Due to MANET limitation, mobile nodes will be faced by extra cost of communication while sending the false data to destination. False data not only absorbed the nodes energy moreover, it can be broken down a network such as denial of service attack. The false reports consume lots of network and computation resources and shorten the lifetime of sensor networks. Hence, to ensure the normal

operation of the system, it is critical to filter false data at forwarding nodes before arriving at the destination(Jeba and Paramasivan 2012).

In this thesis tried to engage the Digital signature algorithm by (NACK) negative acknowledgment method to detect the false data in false route and false injected data with intermediate nodes. DNACK is the modified NACK method which can detect the false data in false route and also false data which injected by an attacker in the communication chain.

The aim of this project is to identify the weakness, strength and the efficiency of en-route filtering on Mobile network. DNACK can be introduced as a good candidate on Risky situation, while the probability of a man in a middle or packet fabrication is high. DNACK also can be presented on Battle filed while the messages' missions need to have a high degree of confidentiality. DNACK method has been discussed deeply in chapter 4 and the results of DNACK method are shown in chapter 5 based on packet delivery percentage and false data detection's time.

1.5 Objectives of the Study

MANET is a type of multi-hop network, infrastructure less and the most important self-organizing. Due to its wireless and distributed nature, there is a great challenge for system security designers. In the last few years, security problems in MANETs have attached much attention; most of the research effort focusing on specific security areas, like securing routing protocols or establishing trust infrastructure or False Data Detection and response.

According to the last researches in MANET FDD that mentioned in Chapter 2, objectives of this research can be partitioned to 3 parts as well as:

1) Study on the existing False Data Detection method on MANET.

2) Implement and develop the most significant detection method. In this thesis the “negative acknowledgment,” (NACK) method has been chosen as a main method.
3) Propose the new enhancement of NACK called DNACK.
4) Compare the efficiency of the proposing method (DNACK) in comparison by chosen the method (NACK)(Sun, Chen et al. 2012).

1.6 Research Questions

A. How messages integrity can be guaranteed in hop-by-hop monitoring system?
B. What are the challenges of the NACK method for false data Detection in MANET?
C. How to enhance the NACK method for having the more confidential communication chins?

1.7 Significance of the Study

This research done, based on the issues of en-route monitoring in 802.11, proposing an optimized technique for reducing mentioned issues. This proposed technique is able to prepare a mobile network environment away from false data threats. The findings of this research are important to enhance the messages’ confidentiality by engaging the digital signature in NACK method.

DNACK can be introduced as a good candidate on Risky situation, while the probability of a man in a middle or packet fabrication is high. DNACK also can be presented on Battlefield while the messages’ missions need to have a high degree of confidentiality. DNACK method has been discussed deeply in chapter 4 and the

results of DNACK method are shown in chapter 5 based on packet delivery percentage and false data detection's time.

1.8 Scope of the Study

This report tries to have a brief illustration on security threats and challenges of false data injection in MANET. There are two main parts of this thesis, in the first part previous research in false data Detection are discussed .Implementation in NS-2.35 would be the second part of this thesis .Result of implementation are compared with the result of existing research in false data detection were proposed by(Sun, Chen et al. 2012) .

The scope of this project is limited to the following

1. The NACK method on DSR routing protocols
2. Using Digital signature algorithm for Messages authentication and verification
3. Efficiency of NACK and DNACK routing method in mobile network
4. The simulation environment will be based on Network Simulator-2(NS-2.35).
5. The evaluations between this two method (NACK and DNACK) based on nodes Delay process, packet delivery ratio, and successful data delivery.

REFERENCES

Abdalla, A. M., I. A. Saroit, et al. (2011). "Misbehavior nodes detection and isolation for MANETs OLSR protocol." Procedia Computer Science 3(0): 115-121.

Ahmad, N. and S. M. Rezaul Hasan (2012). "Efficient integrated AES crypto-processor architecture for 8-bit stream cipher." Electronics Letters 48(23): 1456-1457.

Arom-oon, U. and P. Keeratiwintakorn (2011). The fuzzy path selection for OLSR routing protocol on MANET (based on IPV 6 Over IEEE 802.15.4). Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2011 8th International Conference on.

Azer, M. A., S. M. El-Kassas, et al. (2008). Intrusion Detection for Wormhole Attacks in Ad hoc Networks: A Survey and a Proposed Decentralized Scheme. Availability, Reliability and Security, 2008. ARES 08. Third International Conference on.

Bala Krishna, M. and M. N. Doja (2011). (s_2)Symmetric key management and distribution techniques in wireless ad hoc networks. Computational Intelligence and Communication Networks (CICN), 2011 International Conference on.

Bala Krishna, M. and M. N. Doja (2011). Symmetric key management and distribution techniques in wireless ad hoc networks. Computational Intelligence and Communication Networks (CICN), 2011 International Conference on.

Balakrishna, R., U. R. Rao, et al. "DETECTION OF ROUTING MISBEHAVIOR IN MOBILE AD HOC NETWORKS."

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

Buchegger, S. and J.-Y. Le Boudec (2002). Performance analysis of the CONFIDANT protocol. Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, ACM.

Chan, A. C. F. (2004). Distributed symmetric key management for mobile ad hoc networks. INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies.

Cho, J.-H. and I.-R. Chen (2011). "Performance analysis of hierarchical group key management integrated with adaptive intrusion detection in mobile ad hoc networks." Performance Evaluation **68**(1): 58-75.

Ertaul, L. and W. Lu (2005). ECC based threshold cryptography for secure data forwarding and secure key exchange in MANET (I). NETWORKING 2005. Networking Technologies, Services, and Protocols; Performance of Computer

and Communication Networks; Mobile and Wireless Communications Systems, Springer**:** 102-113.

Forouzan, B. A. (2007). Cryptography & Network Security, McGraw-Hill, Inc.

Gupta, S., S. Kar, et al. (2011). WHOP: Wormhole attack detection protocol using hound packet. Innovations in Information Technology (IIT), 2011 International Conference on.

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

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

Jalil, K. A., Z. Ahmad, et al. (2011). Securing routing table update in AODV routing protocol. Open Systems (ICOS), 2011 IEEE Conference on.

Jeba, S. A. and B. Paramasivan (2012). "AN EVALUATION OF EN-ROUTE FILTERING SCHEMES ON WIRELESS SENSOR NETWORKS." Journal Impact Factor **3**(2): 62-73.

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.

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.

Li, W. and G. Fei (2010). A Secure Clustering Scheme Protocol for MANET. Multimedia Information Networking and Security (MINES), 2010 International Conference on.

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.

Liu, Y., P. Ning, et al. (2009). False data injection attacks against state estimation in electric power grids. Proceedings of the 16th ACM conference on Computer and communications security. Chicago, Illinois, USA, ACM**:** 21-32.

Lu, L., W. Ze, et al. (2011). A Certificateless Key Management Scheme in Mobile Ad Hoc Networks. Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on.

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 on **23**(1): 32-43.

Luo, J., D. Ye, et al. (2009). "A survey of multicast routing protocols for mobile Ad-Hoc networks." Communications Surveys & Tutorials, IEEE **11**(1): 78-91.

Matin, M. A., M. M. Hossain, et al. (2009). Performance evaluation of symmetric encryption algorithm in MANET and WLAN. Technical Postgraduates (TECHPOS), 2009 International Conference for.

Mishra, A., K. Nadkarni, et al. (2004). "Intrusion detection in wireless ad hoc networks." Wireless Communications, IEEE **11**(1): 48-60.

Perrig, A., J. Stankovic, et al. (2004). "Security in wireless sensor networks." Communications of the ACM **47**(6): 53-57.

Rahman, M. and S. Sampalli (2012). A Hybrid Key Management Protocol for Wireless Sensor Networks. Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on.

Selvamani, K., S. Anbuchelian, et al. (2012). A hybrid framework of intrusion detection system for resource consumption based attacks in wireless ad-hoc networks. Systems and Informatics (ICSAI), 2012 International Conference on.

Sen, J. (2010). An Intrusion Detection Architecture for Clustered Wireless Ad Hoc Networks. Computational Intelligence, Communication Systems and Networks (CICSyN), 2010 Second International Conference on.

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.

Su, M.-Y. (2010). "WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks." Computers & Security **29**(2): 208-224.

Sun, C. I., H. Y. Lee, et al. (2009). "A path selection method for improving the detection power of statistical filtering in sensor networks." J. Inf. Sci. Eng **25**: 1163-1175.

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.

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.

Wahengbam, M. and N. Marchang (2012). Intrusion Detection in MANET using fuzzy logic. Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on.

Wang, H. and Q. Li (2007). PDF: a public-key based false data filtering scheme in sensor networks. Wireless Algorithms, Systems and Applications, 2007. WASA 2007. International Conference on, IEEE.

Wang, W., H. Wang, et al. (2013). "Energy-aware and self-adaptive anomaly detection scheme based on network tomography in mobile ad hoc networks." Information Sciences **220**(0): 580-602.

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.

Yang, H., F. Ye, et al. (2005). Toward resilient security in wireless sensor networks. Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, ACM.

Yang, Y., C. Jian, et al. (2009). A self-configuration management model for clustering-based MANETs. Ultra Modern Telecommunications & Workshops, 2009. ICUMT '09. International Conference on.

Ye, F., H. Luo, et al. (2004). Statistical en-route filtering of injected false data in sensor networks. INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, IEEE.

Yun, Z., F. Yuguang, et al. (2008). "Securing wireless sensor networks: a survey." Communications Surveys & Tutorials, IEEE **10**(3): 6-28.

Zhou, L. and Z. J. Haas (1999). "Securing ad hoc networks." Network, IEEE **13**(6): 24-30.

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.