Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X

Vol.3 Issue 4 (2017) 239 - 243. Submitted 25/11/2017. Published 30/12/2017

DYNAMIC NETWORK CONTROL FOR CONFIDENTIAL MULTI HOP COMMUNICATIONS

[1]K.Matheswari, M.Phil Scholar, Department of Computer Science, Bharathiyar Arts and Science College for Women, Deviyakurichi, Thalaivasal, Salem.

[2]K.Anbumathi, Assistant Professor, Department of Computer Science, Bharathiyar Arts and Science College for Women, Deviyakurichi, Thalaivasal, Salem.

Abstract:

Large-scale ad-hoc networks are deployed in numerous application domains, and the data they collect are used in decision making for critical infrastructures. We consider the problem of resource allocation and control of multi-hop networks in which multiple source-destination pairs communicate confidential messages, to be kept confidential from the intermediate nodes. We act the problem as that of network service maximization, into which confidentiality is incorporated as an additional quality of service constraint. Data are streamed from multiple sources through intermediate processing nodes that aggregate information. In this paper, we propose a novel lightweight scheme to securely transmit data. The proposed technique relies on in-packet Bloom filters to encode data. We introduce efficient mechanisms for data verification and reconstruction at the base station. In addition, we extend the secure data scheme with process to detect packet drop attacks execute by malicious data forwarding nodes. We classify the proposed technique both analytically and empirically, and the results prove the effectiveness and efficiency of the lightweight secure data scheme in detecting packet forgery and loss attacks.

Keywords: Packet Drop, Bloom Filter, Lightweight, Packet Forgery Confidentiality.

1. INTRODUCTION

Data are produced at a large number of sensor node sources and processed in-network at intermediate hops on their way to a base station that performs decision-making. The diversity of data sources creates the need to assure the trustworthiness of data, such that only trustworthy information is considered in the decision process. Data provenance is an effective method to assess data trustworthiness, since it summarizes the history of ownership and the actions performed on the data. We investigate the problem of secure and efficient data transmission and processing for sensor networks. In a multi-hop sensor network, data verification allows the base station to trace the source and forwarding path of an individual data packet since its generation. Verification must be recorded for each data packet, but important challenges arise due to the tight storage, energy and bandwidth constraints of the sensor nodes. Therefore, it is necessary to devise a light-weight solution which does not introduce significant overhead. Furthermore, sensors often operate in an untrusted environment, where they may be subject to attacks. Hence, it is necessary to address security requirements such as confidentiality, integrity and freshness of provenance. Our goal is to design a data encoding and decoding mechanism that satisfies such security and performance needs. We propose a data encoding strategy whereby each node on the path of a data packet securely embeds verification information within a Bloom filter, which is transmitted along with the data. Upon receiving the data, the base station extracts and verifies the data. In existing system, confidentiality of communicated information

between the nodes is necessary but the existing system not able to share information to any other node. So they are not providing any confidentiality regarding to the message. Even in scenarios in which confidentiality is not necessary; it may be dangerous to assume that nodes will always remain uncompromised. Keeping different nodes information confidential can be viewed as a precaution to avoid a captured node from gaining access to information from other un-captured nodes. Hence to overcome some drawbacks like to detect if destination change was staged by a malicious node, the confidentially regarding message not intended and recovery of data is not possible. We propose a RSA algorithm for data encoding and data decoding scheme. We design efficient techniques for data decoding and verification at the base station (Destination). We extend the secure data encoding scheme and devise a mechanism that detects packet drop attacks staged by malicious node. We perform a detailed security analysis and performance evaluations of the proposed data encoding scheme and packet loss, packet alter detection mechanism with destination change.

2. RELATED WORK

In the multihop setting, studies the secrecy capacity scaling problem. Exploitation of path diversity in order to achieve secrecy from external eavesdroppers is studied in and for secrecy via mobility. In a method is given that modifies any given linear network code into a new code that is secure requiring a large field size. Later, generalized and simplified the method, and showed that the problem of making a linear network code secure is equivalent to the problem of finding a linear code with certain generalized distance properties.

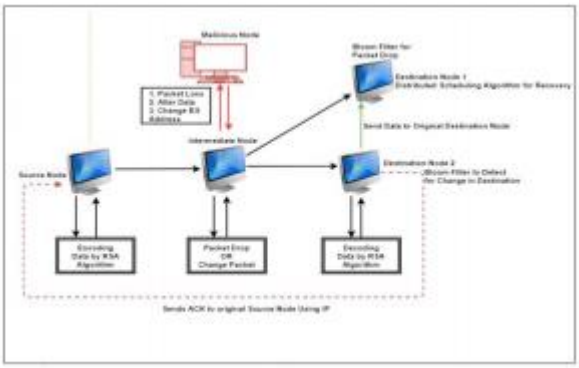

Fig.1.System Model

Along the same lines, investigates secure communication over wireless networks where a node can observe one of an arbitrarily selected collection of secure link sets. In, a different notion of security referred to as packet-level security is used, where it is sufficient that the eavesdropper does not correctly decode the message, i.e., it does not guarantee full equivocation. Recently in, we have investigated the cross-layer resource allocation problem with confidentiality in a cellular wireless network, where users transmit information to the base station, confidentially from the other users. In this paper, we consider a general multi-hop network topology and develop dynamic network control algorithms to jointly determine the end-to-end encoding rates, scheduling and routing. Each source node in aims to keep its information confidential from the nodes in the set of. To that end, a source node precodes its message, divides it into multiple pieces, and sends separate pieces over different paths to the destination. Henceforth, none of the intermediate relay

nodes in the set of will accumulate sufficient amount of information to decode the confidential message, even in part.

3. PROPOSED SYSTEM

A Black Hole attack is a type of routing attack in which malicious node shows itself with a shortest path to destination in a network by sending fake route reply to the source node. The black hole attack is an active insider attack having two properties: first, the attacker consumes the intercepted data packets without forwarding them. Second, the node exploits the mobile ad hoc routing protocol, to pretend itself as having a valid path to a destination node with the intention of intercepting packets. In this attack, malicious node injects fault routing information to the network and leads packets toward itself and then intercepts or discards all of them. In fabrication attack, malicious node destroys routing table of nodes by injecting fault information. Malicious node creates fault routing paths. As a result, nodes send their packets in fault routes. Therefore, network resources wasted, packet delivery rate decreased and packet lost will growth. However, it is also true that a node may easily be stolen and become compromised. Thus, the trust between nodes in ad-hoc networks cannot be guaranteed. Furthermore, this problem may increase the chance to tamper the stolen node. It is also vulnerable since every node in MANET uses radio wave to communicate. It is very hard to detect any node since there is no explicit evidence. Secure routing is an important issue in MANETs. A particularly devastating attack in wireless networks is the black hole attack. The performance of ad hoc networks depends on cooperation and trust among distributed nodes. To enhance security in ad hoc networks, it is important to evaluate trustworthiness of other nodes without centralized authorities. As a result, an efficient algorithm to detect black hole attack is important.

4. ANALYSIS

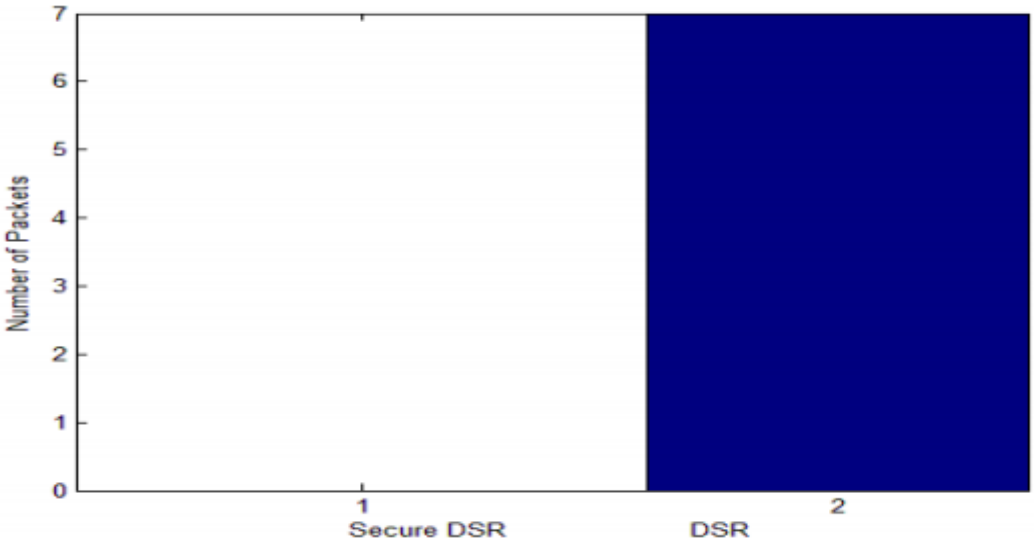

Fig.2.Analysis

The goal of this paper was to provide a simple node based trust management scheme for MANET with multiple perspectives on the concept of trust, an understanding of the properties, which should be considered in developing a trust metric, and insights on how a trust metric can be customized to meet the

requirements and goals of the NTM scheme. Secure routing protocols is a crucial area towards security of MANET.

The routing solutions for conventional networks are not sufficient to work efficiently in ad-hoc environment. In this dissertation, we have proposed a scheme to select secure route for data forwarding. This technique will avoid interception of messages through blackhole nodes. We have compared our results with DSR routing protocol, the results showed that Secure DSR will avoid routing of packets through black hole nodes. The goal of this work is to provide a simple node based trust management scheme for MANET with multiple perspectives on the concept of trust, an understanding of the properties, which should be considered in developing a trust metric, and insights on how a trust metric can be customized to meet the requirements and goals of the NTM scheme. The model is simple, flexible and easy to be implemented. After introducing and analyzing the concept of node-based trust in MANET, we suggested future research directions to develop trust management schemes with desirable attributes such as adaptation to environmental dynamics, scalability and reliability. We propose a dynamic control algorithm associate with end-to-end secrecy encoding, where messages are encoded over infinitely many blocks. Hence, the decoding delay of confidential message may be infinitely long. Unlike the infinite-block case, since a message is encoded across a finite number of blocks, subsequent packets associated with a given secrecy encoded message cannot be decoupled. Therefore, achieving perfect secrecy for all messages is not possible. Hence, we define the notion of secrecy outage. We say that a secrecy outage event occurs, when the confidential message is intercepted by any intermediate node, i.e., the perfect secrecy constraint is violated. First source node will send file to destination then here the sequence number generated as 1.Then the file will pass through intermediate node then the sequence number generated as 2. When data reaches at intermediate node then hacker will drop the data, alter the data or change the destination address then the sequence number generated as 3. Destination node received the data with 3 sequence number. Then destination will get the information that node received the data by 3 sequence number then the node received the data with extra sequence number. Then it will get the information that the malicious node changes the data.

CONCLUSION

Each attacker is capable of tapping into all the information transmitted and received by a single intermediate node. Attackers are not capable of changing the content of the information the node forwards, nor do they inject phantom messages into the network. In our model, intermediate nodes are entities, compliant with network operations as they properly execute algorithms, but the messages need to be kept confidential from them.We addressed the problem of securely transmitting data for sensor networks, and proposed a data encoding and decoding scheme based on Bloom filters. The scheme ensures confidentiality, integrity and freshness of data. We extended the scheme to incorporate data binding, and to include packet sequence information that supports detection of packet loss attacks. Experimental and analytical evaluation results show that the proposed scheme is effective, light-weight and scalable. In future work, we plan to implement a real system prototype of our secure scheme, and to improve the accuracy of packet loss detection, especially in the case of multiple consecutive malicious sensor nodes.

REFERENCES

[1]. Raihana Ferdous, Vallipuram Muthukkumarasamy, Abdul Sattar, "Trust Management Scheme for Mobile Ad-HocNetworks", 2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010).

[2]. Erman Ayday, Hanseung Lee, Faramarz Fekri, "Trust Management and Adversary Detection for Delay Tolerant Networks", 978-1-4244-8180-4/10/$26.00 ©2010 IEEE.

[3]. Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S. Obaidat, "Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks ", 978-1-4244-9268-8/11/$26.00 ©2011 IEEE.

[4]. Isaac Woungang, Mohammed S. Obaidat, Sanjay Kumar Dhurandher, Han-Chieh Chao, Chris Liu, "Trust-Enhanced Message Security Protocol for Mobile Ad Hoc Networks", 978-1-4577-2053-6/12/$31.00 ©2012 IEEE.

[5]. Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.1, February 2012.

[6]. Latha Tamilselvan, Dr. V Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in Manet", Journal Of Networks, Vol. 3, No. 5, May 2008.

[7]. Vishnu K, Amos J Paul, "Detection and Removal of Cooperative Black/Gray hole attack in Mobile AdHoc Networks", 2010 International Journal of Computer Applications (0975 - 8887).