International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Survey of Security Improvement of Dropper Elimination Scheme for IoT Based Wireless Networks

R.Parthiban, S. Usharani, D. Saravanan

Department of CSE, IFET College of Engineering, Villupuram, Tamil Nadu, India

ABSTRACT

Privacy and Security are major issue occur in IoT network. The main objective of the project was to eliminate the eavesdropper collusion occurred by the two or more devices communicating via optimal relay with centralized router using IOT network. To overall delay is reduced with increase in throughput. The security and privacy are some of the major issues that prevent the wide adoption of Internet of Things. This paper studies the important of Received signal strength of wireless communication under eavesdropper collusion where detecting the malicious node. To provide knowledge about the security improvement in wireless communication network by using RSS algorithm.

Keywords : IoT, Signal Strength, MRC, SNR, PHY, MANET, TAS, DSDV, OLSR, AODV ,DSR, TRDSA, BCCE, PPP, GSC

I. INTRODUCTION

An IOT network is built, operated, and maintained by its constituent wireless nodes. These nodes generally have a limited transmission range and so each node seeks the assistance of its neighbouring nodes in forwarding packets. In order, to establish routes between nodes, which are farther than a single hop, specially configured routing protocol is engaged. The unique feature of these protocols is their ability to trace routes in spite of a dynamic topology. These malicious nodes can carry out both Passive and Active attacks against the network.

II. METHODS AND MATERIAL

1. Literature Survey

i) Giovanni Geraci, Jinhong Yuan **"Secrecy Rates in Broadcast Channels with Confidential Messages and External Eavesdropper"**

In this paper, the broadcast channel with confidential messages and external eavesdroppers (BCCE), where a multi-antenna base station simultaneously communicates to multiple potentially malicious users, in the presence of randomly located external eavesdroppers. Using the proposed model, we study the secrecy rates achievable with regularized channel inversion (RCI) pre-coding by performing a large-system analysis that combines results from stochastic geometry and random matrix theory, where the number of users K and the number of transmit antennas N both grow to infinity in a fixed ratio. We obtain explicit expressions for the probability of secrecy outage and an upper bound on the rate loss due to the presence of external eavesdroppers. We show that both these quantities scale as the density of external eavesdroppers grows, irrespective of their collusion strategy. Furthermore, we derive a practical rule for the choice of the regularization parameter, which is agnostic of channel state information and location of eavesdroppers, and yet provides close to optimal performance.

ii)Li Chen, Ying Yang, Guo Wei "Physical Layer Security Enhancement with Generalized Selection Diversity Combining"

In this paper, we present and analyze utilizing generalized selection combining (GSC) scheme to enhance the physical layer (PHY) security of a wireless communication system consisting of a single antenna transmitter, a multi-antennas receiver and a multi-antennas eavesdropper. We consider a practical scenario where GSC scheme is applied to the receiver considering both the complexity and the energy dissipation while maximal ratio combining (MRC) scheme is applied to the eavesdropper in order to maximize its instantaneous signal to noise ratio (SNR). This work bridges the gap between the existing works utilizing MRC scheme and transmit antenna selection (TAS) scheme to enhance the PHY security. Closed-form expressions for both the probability of non-zero secrecy capacity and the exact secrecy outage probability are derived over Rayleigh fading channels. The security capacity performances are also shown and analyzed through numerical results. The impacts of the number of selected branches, the average SNR of transmitter's channel and eavesdropper's channel are discussed.

iii) Ahmed A. Zewail and Aylin Yener "Two-Hop Untrusted Relay Channel with an External Eavesdropper Under Layered Secrecy Constraints"

We consider a Gaussian network consisting of a source that aims to communicate to its legitimate destination via an untrusted relay node in the presence of an external eavesdropper. The source wishes to send two independent messages to the destination: one message must be kept secret from the external eavesdropper only, while the other message must be kept secret from the external eavesdropper and the untrusted relay both. We identify achievable secure rates under these layered secrecy constraints. Considering a two-hop half-duplex setup, we employ the destination as a cooperative jammer in the first phase in order to help provide secrecy from the relay and the external eavesdropper, and the source as a cooperative jammer in the second phase in order to detriment the external eavesdropper. The source encodes its messages using stochastic encoding and security embedding coding. We provide the secrecy analysis and present numerical results to demonstrate the performance of the proposed achievability technique. Our study points to the value of the source serving as a cooperative jammer as well as the need for power control policies at the legitimate nodes in order to ensure secrecy in this system.

iv) Deepika Kukreja,Umang "Trust based Routing using Dominating Set Approach (TRDSA) in Wireless Ad-Hoc Networks"

Secure routing protocols for Mobile Ad hoc Networks (MANETs) have been categorized based on the model used for enforcing security, methodology and information they use to make routing decisions. Some protocols are designed from scratch so as to incorporate security solutions and some are designed to provide security mechanisms into the existing routing protocols like DSDV, OLSR, AODV ,DSR etc. Several protocols for secure routing in ad-hoc networks have been proposed. But due to their limitations, there is a need to make them robust and more secure so that they can go well with the demanding requirements of ad hoc networks. We propose and design a new protocol - Trust based Routing using Dominating Set Approach (TRDSA) which overcomes the shortcomings of existing protocols.

III. EXISTING METHODOLOGIES

a) Broadcast Channel with Confidential Messages and External Eavesdroppers (BCCE)

The spatial location of the external eavesdroppers can be modeled either deterministically or stochastically. There are many important scenarios, only a statistical report of the positions of the eavesdroppers is available, and thus a stochastic spatial model is more suitable. Since these positions are unknown, we treat them as completely accidental according to a homogeneous Poisson point process (PPP). The spatial PPP is a natural choice in such locations because, number of node given and uniformly distributed in the region. The PPP models the most random configuration, and it has extreme entropy among all homogeneous processes. Hence, the PPP attends as a simple and useful model for the site of randomly located nodes in a IoT network.

b) Generalized selection combining (GSC)

Generalized selection combining (GSC), also known as hybrid selection/maximum ratio combining (H-S/MRC), is a additional universal diversity combing which bridges the gap between SC and MRC. The basic idea of GSC is to select a subset of the best diversity paths and then combine them in the MRC fashion in order to reduce the complexity and the energy dissipation of combining schemes. However, to the best of our knowledge, there are no works that considered the PHY security enhancement with GSC at the receiver. In this paper, we consider a practical scenario where GSC scheme is applied to the receiver considering the complexity and the energy dissipation and MRC scheme is applied to the eavesdropper in order to maximize its instantaneous SNR. This work can also be regarded as the generalized formulation of the works considering MRC scheme and SC scheme. Closed-form expressions for the probability of non-zero secrecy capacity and the exact secrecy outage probability are derived.

c) Cooperation Relay Techniques

Role of cooperation with relays under the both afore mentioned confidentiality concerns. We consider a network where a source aims to communicate securely with its destination via an untrusted relay node in the presence of an external eavesdropper. In particular, we wish to investigate the impact of layered secrecy constraints on end-to-end secure communication rates. The source thus aims to send two independent messages to the legitimate destination: the first message must be kept secret from the external eavesdropper, while the second message must be kept secret from the external eavesdropper and the untrusted relay both. Such a model captures the case where the source can trust the untrusted relay for part of the transmitted information but not all of it. Since, we only impose decodability constraints at the legitimate destination, this model differs where there are two legitimate destinations with different levels of security clearance.

d) Trust based Routing using Dominating Set Approach (TRDSA)

TRDSA presents a method for selection of a trustworthy and shortest path between source and destination that is free from malicious nodes. TRDSA is able to detect the malicious nodes inducing attacks like:grayhole, malicious topology change behavior, dropping data packets, dropping control packets, modifying the packet and malicious flooding. The solution also works for attacks induced by colluding malicious nodes. In TRDSA, unlike most of the existing protocols in this area, it requires only few nodes to operate in promiscuous mode which results in the reduction of network overhead as compared to the protocols which requires all the network nodes to work in promiscuous mode. Nodes working in the promiscuous mode persistently require nodes to have high energy capacity as they need to overhear all the transmissions. To select a set of n nodes called Dominating set such that all the nodes in the network are either in the Dominating set or neighbors of the nodes in the Dominating set. From the Dominating set l most trusted nodes (initially trust represents less mobile nodes) that have remaining energy higher than threshold energy required for working in the promiscuous mode are selected.

IV. RESULTS AND DISCUSSION

1. Research Issues

The increasing popularity and usage of wireless technology is creating a need for more secure wireless networks. Wireless networks are particularly vulnerable to a Powerful attack known as the eavesdropper attack. This paper disscuses a new trust based that prevents eavesdropper attacks on a wireless network. A few existing Protocols detect eavesdropper attacks but they require highly specialized equipment not found on most wireless devices. This project aims to develop a defence against Wormhole attacks that does not require as a significant amount of specialized equipment.

2. Solution Domain

There are several simple techniques to detect wormholes in a network but these have some basic flaws which are discussed in the current section.

3. Link Frequency Analysis

Analysis of the link frequency is a simple method to detect a wormhole in a Network. Abnormally high frequency of a link could suggest that it can be a wormhole luring traffic into it. But in the case of cluster networks where the bottleneck links offer comparable delays as that of a wormhole in the network, the traffic might be equally distributed between the bottleneck link and the wormhole link and there is no way to find whether there is a wormhole and if found, it will be difficult to identify the wormhole link.

4. Trust Based Model

Another significant method to detect wormholes is by the use of trust information. Nodes can monitor the behaviour of their neighbour and rate them. Assuming that a wormhole drops all the packets it receives as in blackholes, a wormhole in such a system should have the least trust level and can be easily eliminated. Drops in bottleneck in a network could be due to congestion, which could be triggered by improper routing, high TCP window sizes, sudden bursts of traffic from a node etc. But all these drops occur in bursts and network gets reconfigured after congestion. For example, if there are a lot of drops in TCP, the window size is decreased. Hence, the drop of packets in bottleneck is generally high only during congestion after which it is brought down again.

V. CONCLUSION

In this paper, we have articulated that as more and more IoT based devices get connected to the internet, it results in the extension of the surface area for external eavesdropper attacks. We have also surveyed the literature on the existing methods to protect the IoT infrastructure and summarized these security methods on how they address the security issues in the IoT.We are study about the eavesdropper attack present in network. We proposed received signal strength scheme for eliminate the eavesdropper in the network. We consider the three factor simulate as result provide as below

- ✓ Throughput
- ✓ Average End to End Delay
- ✓ Packet Delivery Ratio