International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
Research Paper
Available online at: www.jrrset.com

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105

Volume 7, Issue 2
February 2019.
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395

Received on: 06.02.2019 Published on: 28.02.2019 Pages : 26 - 30

AN EFFICIENT TRUST ANALYSIS TECHNIQUE IN MANET'S

[1]M.Chitra, [2]V.Ganesh Aravinth, [3]G.Chidhartahan, [4]Dr.R.Latha
[1]Assistant Professor, [2,3]UG Scholar, [4]Principal
KSK College of Engineering and Technology,Kumbakonam
Tamilnadu,India
Corresponding Author: Chitraganesh12@gmail.com

ABSTRACT

An efficient trust analysis technique Show That Increasing The Number Of Access Points Decreases The Average Secrecy Rate Between The Access Point And Its Associated Sink. However, We Find That Increasing The Number Of Access Points First Increases The Overall Average Secrecy Rate, With A Critical Value Beyond Which The Overall Average Secrecy Rate Then Decreases. When Increasing The Number Of Active Sensors, Both The Average Secrecy Rate Between The Sensor And Its Associated Access Point, And The Overall Average Secrecy Rate Decrease. In Contrast, Increasing The Number Of Sinks Improves Both The Average Secrecy Rate Between The Access Point And Its Associated Sink, And The Overall Average Secrecy Rate.

Keywords - Mobile Ad Hoc Network, Trust based Routing, Black Hole attack, Gray Hole Attack

I. INTRODUCTION

THE proliferation of mobile devices has led to the growth of mobile ad hoc networks (MANETs). These networks consist of a group of wireless mobile nodes that dynamically exchange data among themselves without the reliance on any centralized administration or fixed base station. Self-organizing characteristic enables MANETs to be easily established in a wide variety of disparate situations, such as rescue, emergency operations, and battlefield communications. However, mobility and self-organizing characteristics of MANETs cause the change of topology in an unpredictable way. Most of the time, each mobile node with limited transmission range has to seek assistance of its neighboring nodes for data transmissions. As a result, the performance of MANETs largely depends on the reliable routing among nodes. During the last decade, extensive studies have been conducted on routing in MANETs, which led to several mature routing protocols [1-3]. However, all these routing protocols are designed with an assumption that all nodes are fully trusted and willing to cooperate with each other. Thus, they are vulnerable to routing disruption attackers that are not cooperative or disobey the routing rules. There are three types of routing disruption attacks that can be easily launched in MANETs [4]: (1) active black hole attack, (2) passive black hole attack and (3) gray-hole attack. In active black hole attacks, the attackers always claim that they have the shortest path to the destination even if they do not have any proper routing information. Active black hole attackers can attract considerable amount of data packets and drop them silently. In passive black hole attacks, attackers help forwarding routing messages but discard all passing-by data packets. In gray-hole attacks, instead of dropping all passing-by data packets, gray-hole attackers may selectively forward those data packets that can maximize their own interests. In other words, gray-hole attackers may alternatively behave well and badly. However, to our best knowledge, no existing WSNTSs give appropriate solutions to save the energy consumed by the watchdog technique (i.e., the trust-energy conflict induced by watchdog usage has not been addressed before). In particular, some WSNTSs do not discuss how to schedule watchdogs in their proposals while some others implicitly suggest to let sensor nodes launch neighbor-flooding watchdog tasks to monitor all their neighbors and do not study which frequency is appropriate for their monitoring. This kind of neighbor-flooding methods could make running watchdogs redundant and will waste a lot of energy without inducing much additional security benefits. As a result, to simultaneously save energy and collect sufficient past behaviors for trust evaluation, an intelligent watchdog scheduler is highly required.

I. RELATED WORK

Physical layer security has emerged as an appealing low-complexity approach to secure the information transmission. The core idea behind it is to exploit the characteristics of wireless channels such as fading or noise to transmit a message from a source to an intended destination while keeping the message confidential from eavesdroppers. Motivated by this, the potential applications of physical layer security have been investigated in various wireless networks such as cellular networks, cognitive radio, ad-hoc, etc.

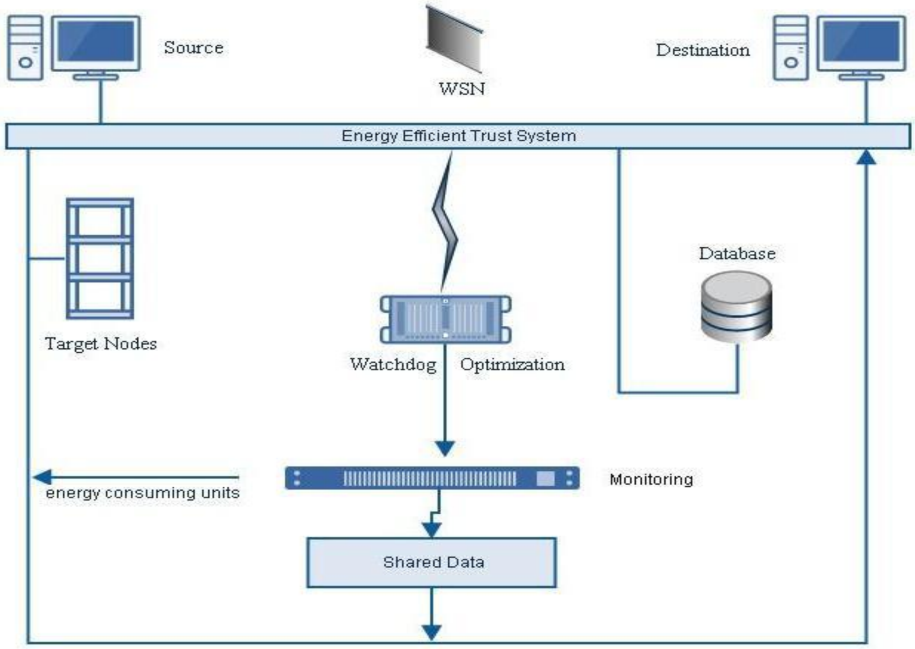
Drawbacks of Existing System

- Providing security in a MANET is a challenging task
- Security solutions for fixed wired networks are not easily adaptable to mobile wireless networks
- A sensor node in a Network may have limited computational resource, running an IDS all the time may turn out to be a costly overhead

II. PROPOSED SYSTEM

In this paper, we fill this gap by optimizing watchdog techniques for WSNTSs to balance energy efficiency and security (in terms of trust accuracy and robustness). Our ultimate goal is to reduce the energy cost induced by watchdog tasks as much as possible, while keeping trust accuracy and robustness in a sufficient level. To touch this goal, we optimize watchdog techniques in two levels. First, we optimize watchdog locations by considering the fact: although sensor nodes which are located more closely may consume less energy to monitor each other due to shorter communication distance, these nodes are more likely of being compromised together and launch collaborative attacks .We therefore explore the optimal watchdog location (given a target node) to minimize the overall risk (in terms of both energy consumption and security). Second, we optimize watchdog frequency and reduce its redundancy. In particular, compared with the sensor nodes whose behaviors are more uncertain, the nodes with more determined trustworthiness (i.e., trustworthy or untrustworthy) may require less watchdog tasks (i.e., lower watchdog frequency) to further investigate.

II. SYSTEM ARCHITECTURE



III. IMPLEMENTATION

Implementation is the stage in the project where the theoretical design is turned into a working system and is giving confidence on the new system for the users that it will work efficiently and effectively. It involves careful planning, investigation of the current system and its constraints on implementation, design of methods to achieve the change over, an evaluation of change over methods. Apart from planning major task of preparing the implementation are education and training of users. The implementation process begins with preparing a plan for the implementation of the system. According to this plan, the activities are to be carried out, discussions made regarding the equipment and resources and the additional equipment has to be acquired to implement the new system. In network backup system no additional resources are needed. Implementation is the final and the most important phase. The most critical stage in achieving a successful new system is giving the users confidence that the new system will work and be effective. The system can be implemented only after thorough testing is done and if it is found to be working according to the specification. This method also offers the greatest security since the old system can take over if the errors are found or inability to handle certain type of transactions while using the new system.

The following are the two entities involved in this project

- ➢ Client
- ➢ Server
- ➢ Router
- ➢ Attacker

Client

- ✓ The Client will Enter the Necessary Details and click Submit Button to Register .After that enter the User Name and Password ,Click Ok to Login.
- ✓ And Click the Upload Button , then Browse the File and Upload it .
- ✓ Here After Set the Path For File Location.

Server

- ✓ Server will Receive the File And Split the File into Packets and also encrypt the File.

Router

- ➢ Run the Router Application
- ➢ In Router You have to select any Node, Like Node1, Node2,Node3,Node4.

Attacker

- ➢ Run the Attacker Program.
- ➢ If attacker will attack the File the Packet will be Verified By the Bit Identity and the Indentified Packets will be Dropped.

Trust System

Client-server computing or networking is a distributed application that partitions watchdog's task between source and target nodes. Often clients and servers operate over a network on separate functionalities. A server machine is a high-performance host that is running one or more tasks which share its resources with nodes.

Watchdogs Technique

All the active nodes in WSN, Once the correct destination router is found, an end-to-end peer connection (TCP or IP) is established to carry end-system. This connection remains active as long as the file requested transferred and it is dynamically shut down when not in use, permitting casual, any-to-any communication without the burden of specifying peer connections in advance. When performing watchdog tasks to monitor routing behavior, the watchdog nodes may waste some watchdog tasks if they miss the target node's forwarding packets due to noises.

Target Nodes

The number of connections to establish between each pair of target node is established between each and every nodes for network communication. From the source node to the destination node and intermediates node must have connection between source nodes after communicate between combinations of multi node each and every node must be link to each other. In multipath data transmission, send the data from source node that means which type of file size and file extension.

Energy Consumption

In proposed a energy-efficient trust model by applying a geographic target nodes to identify trust managers (may save energy due to low storage usage), while implemented an energy watcher to help sensor nodes estimate their neighbor nodes' energy cost for each packet forwarding and thus enable the selection of the most efficient node as their next hop in the route. Moreover, a watchdog's technology is widely used to estimate energy consumed by each task typical free space wireless radio model. In this model, a sensor node's transmitter unit to the main node as file request and then the facts can be sends multiple requested node and DBP algorithms to avoid the WSNTS attacks. The source node sends all type of file, and then enters the data sends from source node to destination node over the network. As well as data must be send from source node to intermediate node automatically in this module the data's are successfully transfer from source to destination without attacks.

IV. CONCLUSION

A hybrid wireless network combining an infrastructure wireless network and a mobile ad-hoc network leverages their advantages to increase the throughput capacity of the system. However, current hybrid wireless networks simply combine the routing protocols in the two types of networks for data transmission, which prevents them from achieving higher system capacity. In this paper, we proposed a Distributed Three-hop Routing (DTR) data routing protocol that integrates the dual features of hybrid wireless networks in the data transmission process. In DTR, a source node divides a message stream into segments and transmits them to its mobile neighbors, which further forward the segments to their destination through an infrastructure network. DTR limits the routing path length to three, and always arranges for high-capacity nodes to forward data. Unlike most existing routing protocols, DTR produces significantly lower overhead by eliminating route discovery and maintenance. In addition, its distinguishing characteristics of short path length, short-distance transmission, and balanced load distribution provide high routing reliability and efficiency. DTR also has a congestion control algorithm to avoid load congestion in BSes in the case of unbalanced traffic distributions in networks. Theoretical analysis and simulation results show that DTR can dramatically improve the throughput capacity and scalability of hybrid wireless networks due to its high scalability, efficiency, and reliability and low overhead. In future any one good algorithm will be used for improve the hybrid network efficiency.

V. FUTURE ENHANCEMENT

The presented paper provides a comparison of different topologies for the wireless sensor network. Cluster based topology and Fusion center based topology are used for the comparison. These topologies are compared on the basis of the two most important factors for a WSN i.e. lifetime and energy efficiency. From the above comparison, it is concluded that Fusion center based topology is more energy efficient in case of uniform distribution of sensors. On the other hand, when the sensors are distributed randomly, cluster based topology proves to be more efficient.

REFERENCE

[1] H Luo, R. Ramjee, P. Sinha, L. Li, and S. Lu. Ucan: A unified cell and ad-hoc network architecture. In Proc. of MOBICOM, 2003.
[2] P. K. McKinley, H. Xu, A. H. Esfahanian, and L. M. Ni.Unicastbased multicast communication in wormhole-routed direct networks.TPDS, 1992.
[3] H. Wu, C. Qiao, S. De, and O. Tonguz. Integrated cell and ad hoc relaying systems: iCAR. J-SAC, 2001.
[4] Y. H. Tam, H. S. Hassanein, S. G. Akl, and R. Benkoczi.Optimal multi-hop cellular architecture for wireless communications.In Proc.Of LCN, 2006.
[5] Y. D. Lin and Y. C. Hsu. Multi-hop cellular: A new architecture for wireless ommunications. In Proc. of INFOCOM, 2000.
[6] P. T. Oliver, Dousse, and M. Hasler. Connectivity in ad hoc and hybrid networks.In Proc. of INFOCOM, 2002.
[7] E. P. Charles and P. Bhagwat. Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers. In Proc.Of SIGCOMM, 1994.
[8] C. Perkins, E. Belding-Royer, and S. Das. RFC 3561: Ad hoc on demand distance vector (AODV) routing. Technical report, Internet Engineering Task Force, 2003.
[9] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks.IEEE Mobile Computing, 1996.
[10] V. D. Park and M. Scott Corson. A highly adaptive distributed routing algorithm for mobile wireless networks.In Proc.Of INFOCOM, 1997.
[11] R. S. Chang, W. Y. Chen, and Y. F. Wen.Hybrid wireless network protocols.IEEE Transaction on Vehicular Technology, 2003.
[12] G. N. Aggelou and R. Tafazolli.On the relaying capacity of nextgenerationgsm cellular networks.IEEE Personal Communications Magazine, 2001.
[13] T. Rouse, I. Band, and S. McLaughlin. Capacity and power investigation of opportunity driven multiple access (ODMA) networks in TDD-CDMA based systems. In Proc. of ICC, 2002.