Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.637 – 647

RESEARCH ARTICLE

ANONYMOUS DETECTION BASED THE NODE COVERAGE AREA USING ENERGY EFFICIENT DYNAMIC KEY ALGORITHM IN MANET

[1]K.Meena, [2]H.Lookman Sithic

[1]Research Scholar, Muthayammal College of Arts and Science

[2]Associate Professor, Muthayammal College of Arts and Science

ABSTRACT- We have used a Distributed Time Sequence Routing protocol (DTSR); The DTSR is used to locate the correct relay node and sink node for data transmission. In our wireless network is considered in to neighbor's node in the network. Using the node data will be sending in to source to destination. To reduce the energy cost, nodes are active only during data transmission and the intersection of node creates a larger merged node. Then we recognize a particular set of adhoc network applications so as to are flexible to this scalability limit. The Energy efficient dynamic key Exchange is one of the more popular and interesting methods of key distribution. It is a public-key cryptographic system whose sole purpose is for distributing keys, whereby it is used to exchange a single piece of information, and where the value obtained is normally used as a session key for a private-key scheme. The key distribution to adhoc nodes is done by means of two layer process. This paper proposes a key distribution scheme, based on intrusion detection method for using a data transmission from source to destination on the network. It based high level security and more energy efficient data transmission on their network.

Key words: DTSR, adhoc, relay node, sink node

I. INTRODUCTION

Adhoc network are an emerging technology with a wide range of potential applications such as environment monitoring, earthquake detection, patient monitoring systems, etc. Adhoc networks are also being deployed for many military applications, such as target tracking,

surveillance, and security management. Adhoc network typically consist of small, inexpensive, resource constrained devices that communicate among each other using a multi hop wireless network. Each node, called an Adhoc Node, has one adhoc, embedded processors, limited memory, and low-power radio, and is normally battery operated. Each adhoc node is responsible for sensing a desired event locally and for relaying a remote event sensed by other adhoc nodes so that the event is reported to the end user.

MANET is a self-configuring network of mobile nodes connected by wireless links. It is an infrastructure-less system having no designated access points or routers. It follows a distributed architecture and has a dynamic topology in which each node can move randomly in an area of operation. Here each node is free to move independently in any direction, and therefore will change its links to other nodes frequently. Each intermediate node is also a router and forwards traffic sent by other nodes in the path. A popular routing technique for MANET is the Ad Hoc On demand Distance Vector routing protocol, which is a reactive or source initiated on-demand protocol. Compared to the proactive or table driven approaches, these protocols eliminate the need to periodically flood the network with the table updated messages that are required in the table driven approaches.

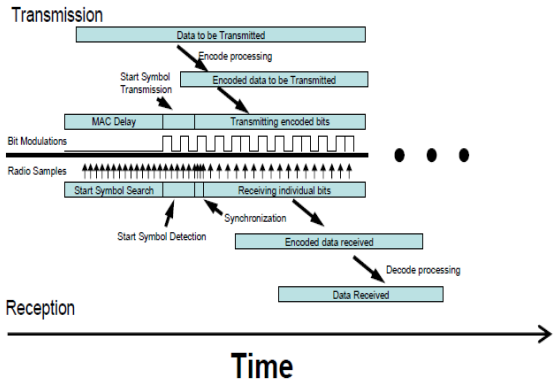


FIG 1. Architecture Diagram for Adhoc network

II. RELATED WORKS

Anonymous Location:

Several direction-finding protocol studies are base on node lifetime and link lifetime. The major object here is to evaluate the node time and the link lifetime utilize the lively nature, such as the energy drain rate in addition to the relative mobility opinion rate of nodes. These two presentation metrics are included by route lifetime-prediction algorithm. This algorithm is approved out as follow select the least lively route with the best lifetime for unrelenting data forward. Node Lifetime in addition to link lifetime forecast methods, the exponentially weighted moving average technique is used to approximation the energy use up rate. The handset can measure the symbol strength when it receives the packet from dispatcher in same power level and then it calculates the distance stuck between two nodes by apply the radio spread model.

A mobile ad hoc network consists of many mobile nodes that can communicate with each other directly or through intermediate nodes. Often, hosts in a manet operate with batteries and

can roam freely, and thus, a host may exhaust its power or move away, giving no notice to its neighboring nodes, causing changes in network topology.

The proposed algorithm consists of the following three phases Route discovery, Data forwarding, and Route maintenance. There are seven main differences between the EDNR and the AODV. First, in the EDNR protocol, every node saves the received signal strength and the received time of the RREQ packet in its local memory and adds this information into the RREP packet header in a piggyback manner when it receives the RREP for the corresponding RREQ packet to meet the requirement of the connection lifetime-prediction algorithm. Second, node agents need to update their predicted node lifetime during every period. Third the node-lifetime information in the RREP packet is updated when the RREP packet is returned from a destination node to the source node.

The main contribution of this paper is that we combine node lifetime and route lifetime-prediction algorithm, which explores the dynamic nature of mobile nodes the energy drain rate of nodes and the relative mobility estimation rate at which adjacent nodes move apart in a route-discovery period that predicts the lifetime of routes discovered, and then, we select the longest lifetime route for persistent data forwarding when making a route decision. The proposed route lifetime-prediction algorithm is implemented by an exploring dynamic nature routing protocol with large scale environment based on quadrant based dynamic source routing.

Anonymity

MANET is a self-configuring network of mobile nodes connected by wireless links. It is an infrastructure-less system having no designated access points or routers. Each intermediate node is also a router and forwards traffic sent by other nodes in the path.

Due to topology changes caused by nodes' mobility in MANET, the routes get disconnected frequently. The existing AODV based routing protocols perform route repair scheme to repair the disconnected route. However, in most cases a source node unnecessarily performs re-route discovery of the whole path even when just one node moves out of the path. Also, if there are no checks on the selection of nodes while performing route discovery there is every possibility that a malicious node may make place in the route leading to a type of attack called the black hole attack. As far as our knowledge goes, there is no such proposed technique in the literature that takes care of both link failure and black hole attack at the same time.

Trust Module

Manet's performance can degrade significantly due to selfish or malicious activities of its nodes. To combat this misbehavior in such dynamic self-organizing networks, a trust management scheme must be introduced. This trust management module plays an important role to improve the performance of the MANET and it provides a secure environment. Similar to the trust management performs the trust evaluation process in three phases: initial phase, update phase, and re-establishment phase. If a new node enters into the network, the neighbor nodes start monitoring the node by initializing the metrics and vice versa. Subsequently some of the nodes may move out of the radio range and also may re-enter later.

Since to restrict or stop using location information is not a solution to the problem, we expect to address the location privacy issue, while still exploiting location to achieve efficiency in routing functionality. Our solution tries to circumvent those difficulties by dissociating location information with identity.

Local Location Update

Each node periodically updates its current location to neighbors along with its identity, which enables the building up of a neighbor table at each node. Remote location update each node periodically updates its current location with identity to remote location servers according to a specific location service algorithm, and reactively responds to location requests. Location request a source node that does not have the location of the intended destination initiates a LREQ message to the corresponding server obtained by the specific Location service algorithm. A message attaches the location and identity of the source so that the response of requested location could reach the original requester. Data delivery during the data forwarding process, each packet attaches the location and identity of the destination so that geographic forwarding strategies could be applied and the intended destination could receive its data.

However, we will only consider the general case in this paper, and we assume that location itself is not enough to derive its subject.

Anonymous Position Service

Another important component for a complete geographic routing scheme is location service that we have not yet discussed so far. In case the source node does not know the location of the destination, it should be able to retrieve it through a location service. However, to achieve an anonymous location service is very challenging as well. In this section, we propose a scheme based on data. In data the network is divided into grids of the same size. Each node could determine some special grids, where its location servers are, by mapping its uniqueness to it.

Our designed anonymous place service attempts to dissociate a node's spot and its identity but does not supply updater anonymity in conditions of hiding its identity. The basic design is that the updater will encrypt its site and its identity earlier than sending it to the location server, and the latent location requester can recover it and decrypt it to find the location. The whole development of location updating and querying will not concurrently expose the position and identity of several of the three parties. For effortlessness, only three nodes A, B and A's position attendant S are involved in this occurrence. Before we discuss how the plan works, we initiate basic notations used in our design.

The method avoids the explicit experience of both position and identity in a usual position service. However, the updating swelling has to spot all its possible senders and has to keep informed the position server accordingly. Otherwise, a few nodes may not be bright to reach it.

Alert Exposures

The locality of a message's correspondent may be open by merely exposing the transmission track. Therefore, an anonymous message protocol that can supply UN traceability is wanted to strictly make certain the anonymity of the correspondent when the sender communicates with the extra side of the field. in addition, a malicious observer could try to block the facts packets by compromising a digit of nodes, stop the packets on a number of nodes, or even copy back to the sender by detecting the information transmission way. Therefore, the direction should also be undetectable.

A malevolent observer may also attempt to detect destination nodes through transfer analysis by launching an intersection bother. Therefore, the target node also needs the shield of anonymity. In this work, the attackers can be battery motorized nodes that inactively receive complex packets and sense activities in their neighborhood.

There may also be lots of nodes for an attacker to take note, so the computing slide is not acceptable, and the triumph rate is low. To extra make it more hard for an attacker to compute the times tamp, we can add to the computation difficulty by using randomization for the instance stamps. Purposely, we keep the accuracy of time stamp to a certain extent, say next, and randomize the digits within complex.

Objectives

The One of the main reasons is the security issue which is discussed in this paper. The secure initialization of a new joining node with network and security parameters to be trusted and to be able to participate actively in the MANETs Security for dynamic address allocation service in MANETs is still an open issue. This paper proposes a security framework to thwart all possible attacks related to the buddy system based proposed protocol called LAR (Location Aided Routing) is based on a fully distributed and a threshold based certified lake address allocation model. While LAR is deployed, the increasing in communication transparency and latency is fairly reasonable then it's also used to dynamic based allocation protocol. Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols that conceal node identity and/or routes from exterior observers inside order to give anonymity protection. However, obtainable anonymous routing protocols relying on either hop-by-hop encryption or outmoded traffic either make high cost or cannot provide full secrecy protection to data sources, destinations, and routes.

The high cost exacerbates the inherent reserve constraint problem in MANETs especially in compact disk wireless applications

MODULE DESCRIPTION

Distributed Time Sequence Routing:

Distributed Time Sequence Routing protocol has used to send the data efficiently and quickly on to their network. In this algorithm to find out the correct node locate route as well as direct path in the network base on the time. DTSR protocol is to transfer the data in to without any modification. Availability parameters mean connectivity and functionality in the network management layer. Connectivity is the physical connectivity of network elements. Loss is the fraction of packets lost in transit from sender to target during a specific time interval, expressed in percentages. Have to improve the network throughput, Network delivery ratio, and availability, data loss.

Consequently, the Energy efficient dynamic key algorithm should be used with a form of authentication such as certificates to ensure that symmetric keys are established between nodes. The steering metrics are evaluated in dissimilar literatures to indicate the significance and measuring purpose of frequent routing protocols.

Keying Process:

In practice, this means that the mobile devices must run a protocol to authenticate each other and to protect the data they exchange (to ensure confidentiality and integrity); the latter operation typically requires setting up a symmetric shared key. This key can be used to secure both immediate communications and communications that take place afterwards. It is a common belief that peer-to-peer security is more difficult to achieve than traditional security based on a central authority;

Synchronization of Multiple Nodes

Adhoc networks most often have a much more complicated topology than the simple examples and not all adhoc nodes can communicate with each other directly. Thus, multi-hop synchronization is required, which adds an additional layer of complexity. Clearly, this could be avoided by using an overlay network which provides virtual, single-hop communication from every adhoc node to a single master node.

Energy Efficient Dynamic Key Algorithm

It should be complemented with an authentication mechanism. In this approach for key distribution in security factors with respect fact that solving attacking problem is very challenging and that the shared key is never itself transmitted over the channel.

Distributed Time Synchronization Routing Protocol

DTSR is a reactive time sync protocol, which can be used to obtain times of event detections at multiple observers in the local time of the sink node(s). We provide a more detailed description of the protocol later when formally analyze the time sync errors it introduces.

III.LITERATURE REVIEW

Design and implementation of a Trust-aware routing protocol for large Adhoc networks

The domain of Wireless Adhoc Networks (Adhoc networks) applications is increasing widely over the last few years. As this new type of networking is characterized by severely constrained node resources, limited network resources and the requirement to operate in an ad hoc manner, implementing security functionality to protect against adversary nodes becomes a challenging task. In this present a trust-aware, location-based routing protocol which protects the adhoc network against routing attacks, and also supports large-scale Adhoc networks deployments.

Precise time synchronization based on ripple flooding in wireless adhoc networks

Precise time synchronization is inevitable for duty-cycling and TDMA in wireless adhoc networks. To achieve a precise synchronized clock between nodes, fast distribution of time information of a reference node to all other nodes in multi-hop without a scheduling is necessary.

Trust Evaluation Based Security in Wireless Adhoc Network

The multi-hop routing in wireless adhoc networks offers little protection against identity deception through replaying routing information. An adversary can exploit this defect to launch various harmful or even devastating attacks against the routing protocols, including sinkhole attacks, wormhole attacks and Sybil attacks. The situation is further aggravated by mobile and harsh network conditions. Traditional cryptographic techniques or efforts at developing trust-aware routing protocols do not effectively address this severe problem. To secure the Adhoc networks against adversaries misdirecting the multi-hop routing, that has been designed and implemented TARF, a robust trust-aware routing framework for dynamic Adhoc networks.

LSR Protocol Based on Nodes Potentiality in Trust and Residual Energy for Adhoc networks

In Wireless Adhoc Networks (Adhoc networks), all the nodes selected for packet routing must be trustworthy, and at the same time energetic too. Smooth conservation of nodes energies and the trust levels, are an important issues in adhoc network because they directly affects the life span and reliability of the nodes as well as the entire network. The energy utilization at every node must be very smooth and at the same time, packets should be forwarded via trusted nodes only. In this paper, we propose an Energy Efficient Link State Routing Protocol (EELSRP) using the potential nodes selected by applying the fuzzy logic on the trust and residual energy levels.

Routing Security Issues in Wireless Adhoc Networks: Attacks and Defenses

The design and implementation of secure Adhoc networks must simultaneously address several difficult research challenges. First, wireless communication among the adhoc nodes increases the vulnerability of the network to eavesdropping, unauthorized access, spoofing, replay, and denial-of-service (DoS) attacks. Second, the adhoc nodes themselves are highly resource-constrained in terms of limited memory, CPU, communication bandwidth, and especially battery life.

Time Synchronization and Calibration in Wireless Adhoc Networks

Physical time plays a crucial role for many adhoc -network applications. While many traditional applications of time also apply to adhoc networks, we will focus here on areas specific to adhoc networks. Its illustrates a rough classification of applications of physical time: at the interface between the adhoc network and an external observer, among the nodes of the adhoc network, and at the interface between the adhoc network and the observed physical world. The following paragraphs will discuss applications of time in these three domains.

IV. PROPOSED SYSTEM

Distributed Time Sequence Routing protocol has used to send the data efficiently and quickly on to their network. In this algorithm to find out the correct node locate route as well as direct path in the network base on the time.

DTSR protocol is to transfer the data in to without any modification. Availability parameters mean connectivity and functionality in the network management layer. Connectivity is the physical connectivity of network elements. Loss is the fraction of packets lost in transit from sender to target during a specific time interval, expressed in percentages.

V. RESULTS AND DISCUSSION

Networks allow computers, and hence their users, to be connected together. They also allow for the easy sharing of information and resources, and cooperation between the devices in other ways. Some of the major benefits are:

Connectivity and Communication:

Networks connect computers and the users of those computers. Individuals within a building or work group can be connected into LAN.

Data Sharing:

One of the most important uses of networking is to allow the sharing of data. True networking allows thousands of employees to share data much more easily and quickly.

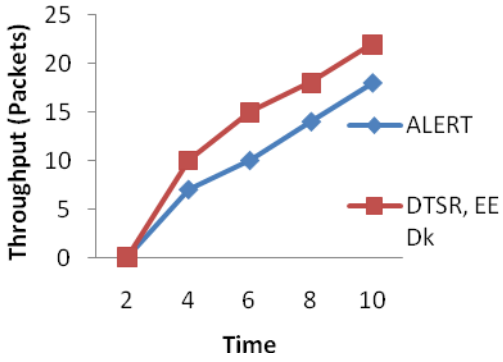
Hardware Sharing:
Networks facilitate the sharing of hardware devices. For example, instead of giving each of 10 employees in a department an expensive color printer, one printer can be placed on the network for everyone to share.

Internet Access:
The Internet is itself an enormous network. The significance of the Internet on modern society is hard to exaggerate, especially for technical fields.

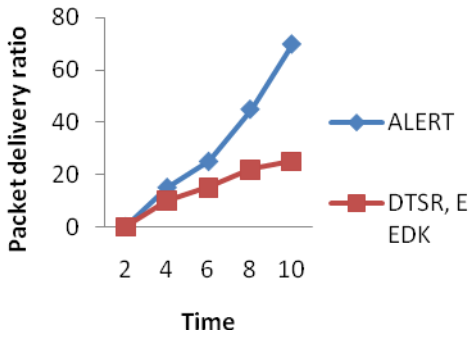
Internet Access Sharing:
Small computer networks allow multiple users to share a single Internet connection. Special hardware devices allow the bandwidth of the connection to be easily allocated to various individuals as they need it.

Data Security and Management:
In a business environment, a network allows the administrators to much better manage the company's critical data. Instead of having this data spread over dozens or even hundreds of small computers in a haphazard fashion as their users create it.

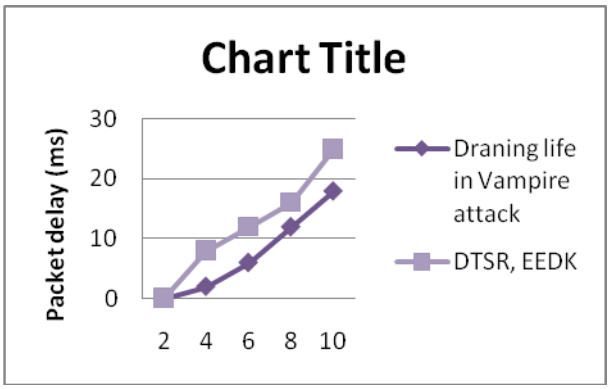
Throughput Performance:-



Packet Delay:



The Packet Delivery Fraction:



VI. CONCLUSION

Then the information based metric, entropy, is applied for final filtering of suspicious flow. Trust value for a client is assigned by the server based on the access pattern of the client and updated every time when the client contacts the server. Energy efficient dynamic key swap is one of the more well-liked and interesting method of key sharing. It is a public-key cryptographic system whose sole reason is for distributing keys, whereby it is used to swap over a single piece of information, and anywhere the value obtained is in general used as a sitting key for a private-key system It enables that adhoc nodes can converse each other securely. Our future work implements the security level based data transmission on network. It carries an expandable range of information resources and services which lead to bulk exchange of traffic over the collision every day. This excessive popularity creates some troubles in the networks. Among them, Node and Diffe Hellman key are the two major events. Web services needs stability and security from these two concerns. There are some methods that can discriminate DDoS attack from node and trace the sources of the attack in huge volume of network traffic. However, it is difficult to detect the exact sources of attacks in network traffic when flicker crowd event is also present. Due to the alikeness of these two anomalies, attacker can easily mimic the malicious flow into legitimate traffic patterns and defense system cannot detect real sources of attack on time. Also to implement the Entropy variation is a theoretic concept which is a measure of changes in concentration of distribution of flows at a router for a given time duration. In future work simulation criteria for considering the resolution of specified objectives and their problem reports simultaneously, that is, the behavior of routing protocols in wireless sensor network by considering the realistic attack traces. The three metrics of Packet delivery ratio, End to end Delay and Throughput are evaluated using AODV protocol in three density regions of low density, medium density and high density in network scene as well as in node point.

REFERENCES

[1]. Qiang Tang, Liqun Chen, "Weaknesses in two group Energy efficient dynamic keykey exchange protocols" 2006
[2]. John Paul Walters, Zhengqiang Liang, "Wireless Sensor Network Security: A Survey" 2006
[3].Aniket Kate, Greg Zaverucha, and Urs Hengartner, "Anonymity and Security in Delay Tolerant Networks" 2008

[4].Mario ˇCagalj, Srdjan ˇCapkun and Jean-Pierre Hubaux, "Key agreement in peer-to-peer wireless networks"
[5].Jean-Fran¸cois Raymond and Anton Stiglic, "Security Issues in the Energy efficient dynamic keyKey Agreement Protocol" 2008
[6].Sye Loong Keoh, Emil Lupu and Morris Sloman, "Securing Body Sensor Networks: Sensor Association and Key Management" 2010
[7].Yongdae Kim_, Adrian Perrig_, and Gene Tsudik, "Tree-based Group Key Agreement" 2011
[8].Victor C. Zandy and Barton P. Miller, "Reliable Network Connections" 2010
[9].Wenliang Du, Jing Deng, Yunghsiang S. Han, "A Key Pre-distribution Scheme for Sensor Networks Using Deployment Knowledge" 2004
[10].Tony Chung and Utz Roedig, "DHB-KEY: An Efficient Key Distribution Scheme for Wireless Sensor Networks" 2008

Author's Details:

H.Lookman Sithic received his B.Sc degree from Bharathidasan University Trichy and M.S. (IT) degree from Bharathidasan University. He has completed his M.Phil at Periyar University. He is having 13 year s of experience in collegiate teaching and he is the Assistant Professor of computer science and applications in Muthayammal college of Arts and Science, Rasipuram affiliated by Periyar University. His main research interests include data mining, Network security.

K.Meena received her B.Sc, degree in Tirupur Kumaran college for women, Tirupur Bharathiyar University, (2000 - 2003) [Tamil Nadu (India)]. Then, did MCA degree in Muthayammal college of Arts and Science, Rasipuram. Periyar University, Salem (2008-2011). She is the M.Phil Research Scholar of Muthayammal College of Arts and Science, Rasipuram. Periyar University, Salem. Her Area of interest is Networking.

