ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. II, Issue IV, April 2016.

ESTABLISHING STABLE AND RELIABLE ROUTING IN HETEROGENIOUS MULTIHOP WIRELESS NETWORKS

M.Ajitha (PG Scholar)

DEPARTMENT OF COMMUNICATION AND NETWORKING

SARDAR RAJA COLLEGE OF ENGINEERING,Alangulam.

Smajicse1@gmail.com

ABSTRACT

E-STAR for establishing stable and reliable routes in heterogeneous multihop wireless networks. E-STAR combines payment and trust systems with a trust-based and energy-aware routing protocol. The payment system rewards the nodes that relay others packets and charges those that send packets. The trust system evaluates the nodes competence and reliability in relaying packets in terms of multi-dimensional trust values. The trust values are attached to the nodes public-key certificates to be used in making routing decisions. I have used two routing protocols to direct traffic through those highly-trusted nodes having sufficient energy to minimize the probability of breaking the route. By this way, E-STAR can stimulate the nodes not only to relay packets, but also to maintain route stability and report correct battery energy capability. This is because any loss of trust will result in loss of future earnings. Moreover, for the efficient implementation of the trust system, the trust values are computed by processing the payment receipts. Analytical results demonstrate E-STAR can secure the payment and trust calculation without false accusations. Simulation results demonstrate that my routing protocols can improve the packet delivery ratio and route stability.

1.1 INTRODUCTION

MULTIHOPWIRELESS NETWORKS

In cellular and wireless local area networks, wireless communication only occurs on the last link between a base station and the wireless end system. In multi-hop wireless networks there are one or more intermediate nodes along the path that receive and forward packets via wireless links. Multi-hop wireless networks have several benefits: Compared to networks with single wireless links, multi-hop wireless networks can extend the coverage of a network and improve connectivity. Moreover, transmission over multiple short links might require less transmission power and energy than over long links. Moreover enable higher data rates resulting in higher throughput and more efficient use of the wireless medium. Multi-hop wireless networks avoid wide deployment of cables and can be deployed in a cost-efficient way. In case of dense multi-hop networks several paths might become available that can be used to increase robustness of the network.Unfortunately, protocols developed for fixed or cellular networks as well as the Internet are not optimal for multi-hop wireless networks. This is in particular the case for routing protocols, where completely new unicast, multicast, and broadcast routing protocols have been developed for mobile ad-hoc and sensor networks.

On the transport layer, the Transmission Control Protocol is the de facto standard in the Internet and in order to allow interoperability, TCP must be

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. II, Issue IV, April 2016.

supported in multi-hop wireless networks as well. However, many protocol mechanisms such as congestion control and error control based on acknowledgements do not work efficiently in multi-hop wireless networks due to various reasons such as contention and control packet overhead. Even on application level new concepts are required to support discovery of available applications and services. Several concrete application scenarios for multi-hop wireless networks have been investigated during the last years. Initially, it has been proposed to deploy multi-hop networks to extend the coverage of cellular networks by relaying packets. Recently, wireless mesh networks have been proposed to provide broadband Internet services without the need of expensive cable infrastructures, in particular in areas sparsely populated. Wireless mesh networks consist of mesh routers and mesh clients, where mesh routers have minimal mobility and form the backbone of wireless mesh networks . It make use of heterogeneous network technology such as IEEE 802.11, 802.16, and cellular radio networks.

Relaying nodes can also be mobile such as in case of vehicles. In that case the term mobile ad-hoc network is more appropriate. Vehicular networks as a special case of mobile ad-hoc networks make use of the frequently existing communication equipment in cars. Wireless sensor networks are another emerging technology, can cover large geographical areas, and provide connectivity without having direct physical access to each sensor node. Sensor nodes can be configured and sensor data can be read using multi-hop networking.

A wireless network enables people to communicate and access applications and information without wires. This provides freedom of movement and the ability to extend applications to different parts of a building, city, or nearly anywhere in the world. Wireless networks allow people to interact with e-mail or browse the Internet from a location thatprefer.Many types of wireless communication systems exist, but a distinguishing attribute of a wireless network is that communication takes place between computer devices. These devices include personal digital assistants , laptops, personal computers , servers, and printers. Computer devices have processors, memory, and a means of interfacing with a particular type of network. Traditional cell phones don't fall within the definition of a computer device; however, newer phones and even audio headsets are beginning to incorporate computing power and network adapters. Eventually, most electronics will offer wireless network connections.As with networks based on wire, or optical fiber, wireless networks convey information between computer devices. The information can take the form of e-mail messages, web pages, database records, streaming video or voice. In most cases, wireless networks transfer data, such as e-mail messages and files, but advancements in the performance of wireless networks is enabling support for video and voice communications as well.

1.1.1 Multi-Hop Networking

In Multi-hop, wireless networks use two or more wireless hops to convey information from a source to a destination. There are two distinct applications of multi-hop communication, with common features, but different applications[10].

1.1.2 Mobile ad hoc networks

A mobile ad hoc network consists of a group of mobile nodes that communicate without requiring a fixed

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. II, Issue IV, April 2016.

wireless infrastructure. In contrast to conventional cellular systems, there is no master-slave relationship between nodes such as Òbase station to mobile usersÓ in ad hoc networks. Communication between nodes is performed by direct connection or through multiple hop relays. Mobile ad hoc networks have several practical applications including battlefield communication, emergency first response, and public safety systems. Despite extensive research in networking, many challenges remain in the study of mobile ad hoc networks including development of multiple access protocols that exploit advanced physical layer technologies like MIMO and interference cancellation, analysis of the fundamental limits of mobile ad hoc network capacity, practical characterization of achievable throughputs taking into account network overheads[4].

1.1.3 Multi-hop cellular networks

Cellular systems conventionally employ single hops between mobile units and the base station. As cellular systems evolve from voice centric to data centric communication, edge-of-cell throughput is becoming a significant concern. This problem is accentuated in systems with higher carrier frequencies and larger bandwidth. A promising solution to the problem of improving coverage and throughput is the use of relays. Several different relay technologies are under intensive investigation including fixed relays .There has been extensive research on multi-hop cellular networks the last few years under the guise of relay networks or cooperative diversity. The use of relays, though, impacts almost every aspect of cellular system design and optimization including: scheduling, handoff, adaptive modulation and interference management.Themultihop packet transmission can extend the network coverage area using limited power and improve area spectral efficiency. In developing and rural areas, the network can be deployed more readily and at low cost. To consider the civilian applications of multihop wireless networks, where the nodes have long relation with the network and also consider heterogeneous multihop wireless networks , where the nodes' mobility level and hardware/energy resources may vary greatly. HMWNs can implement many useful applications such as data sharing and multimedia data transmission.The nodes are typically autonomous and self-interested and may belong to different authorities. The nodes also have different hardware and energy capabilities and may pursue different goals. In addition, malfunctioned nodes frequently drop packets and break routes due to faulty hardware or software, and malicious nodes actively break routes to disrupt data transmission.

1.2 TYPES OF WIRELESS NETWORKS

There are different types are available in the wireless networks,They are some following

1.2.1 Wireless Personal Area Network

A wireless personal area network is a personal area network a network for interconnecting devices centered on an individual person's workspace in which the connections are wireless. Wireless PAN is based on the standard IEEE 802.15. The two kinds of wireless technologies used for WPAN are Bluetooth and Infrared Data Association.A WPAN could serve to interconnect all the ordinary computing and communicating devices that many people have on their desk or carry with them today; or it could serve a more specialized purpose such as allowing the surgeon and other team members to communicate during an operation.A key concept in WPAN technology is known as

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. II, Issue IV, April 2016.

"plugging in". In the ideal scenario, when any two WPAN-equipped devices come into close proximity or within a few kilometers of a central server can communicate as if connected by a cable. Another important feature is the ability of each device to lock out other devices selectively, preventing needless interference or unauthorized access to information.

1.2.2 Wireless LAN

A wireless local area network is a wireless computer network that links two or more devices using a wireless distribution method within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local coverage area and still be connected to the network, and can provide a connection to the wider Internet. Most modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name.Wireless LANs have become popular in the home due to ease of installation and use, and in commercial complexes offering wireless access to their customers; often for free. New York City, for instance, has begun a pilot program to provide city workers in all five boroughs of the city with wireless Internet access.

A peer-to-peer network allows wireless devices to directly communicate with each other. Wireless devices within range of each other can discover and communicate directly without involving central access points. This method is typically used by two computers so that can connect to each other to form a network. This can basically occur in devices within a closed range.If a signal strength meter is used in this situation, it may not read the strength accurately and can be misleading, because it registers the strength of the strongest signal, which may be the closest computer[2].

Hidden node problem: Devices A and C are both communicating with B, but are unaware of each other IEEE 802.11 defines the physical layer and Media Access Control layers based on Carrier Sense Multiple Access with Collision Avoidance. The 802.11 specification includes provisions designed to minimize collisions, because two mobile units may both be in range of a common access point, but out of range of each other.

1.2.3 Wireless mesh network

A wireless mesh network is a communications network made up of radio nodes organized in a mesh topology. It is also a form of wireless ad hoc network. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways which may, but need not, connect to the Internet. The coverage area of the radio nodes working as a single network is sometimes called a mesh cloud. Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network. A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. Wireless mesh networks can self form and self heal. Wireless mesh networks can be implemented with various wireless technology
including 802.11, 802.15, 802.16, cellular technologies or combinations of more than one type.

A mesh network is a network topology in which each node relays data for the network. All mesh nodes cooperate in the distribution of data in the network.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. II, Issue IV, April 2016.

1.2.4 Wireless MAN

A metropolitan area network is a computer network larger than a local area network, covering an area of a few city blocks to the area of an entire city, possibly also including the surrounding areas. A Wireless Metropolitan Area Network is also known as a Wireless Local Loop . WMANs are based on the IEEE 802.16 standard.

Wireless local loop can reach effective transfer speeds of 1 to 10 Mbps within a range of 4 to 10 kilometres, which makes it useful mainly for telecommunications companies.The best-known wireless metropolitan area network is WiMAX, which can reach speeds on the order of 70 Mbps over a radius of several kilometers.

1.2.5 Wireless WAN

A wireless wide area network is a form of wireless network. The larger size of a wide area network compared to a local area network requires differences in technology. Wireless networks of all sizes deliver data in the form of telephone calls, web pages, and streaming video.A WWAN often differs from wireless local area network(WLAN) by using mobile telecommunication cellular network technologies such as LTE, WiMAX, UMTS, CDMA2000,GSM, cellular digital packet data and Mobitex to transfer data.

WWAN services are typically delivered to smart phones and other handheld devices sold bycellular service providers and their retail partners but other mobile devices can use them as well. Some netbooks are available with WWAN cards installed; you can also purchase wireless WAN cards to install yourself. UnlikeWi-Fi cards, which can be used in just about anyhotspot, WWAN devices must be provisioned specifically for access to your service provider's network.Service provider will take care of billing for roaming access that involves other provider networks[10].

1.2.6 Global area network

BGAN was developed to provide cost-effective connectivity in remote locations where cellularand wireless data networks do not currently exist . The system works anywhere on the planet, in fact, but the regions immediately surrounding the north and south geographic poles. Regional BGAN is currently deployed across Europe; the global BGAN system is expected to be fully operational by the middle of 2006. BGAN terminals are capable of supporting multiple users, and will support data, voice, Bluetooth, Ethernet, and Wi-Fi. The electrical power may come from utility lines, batteries, or generators. Connection speeds will be up to approximately 500 kbps, depending on the type of terminal. In contrast to most geostationary satellite communications systems, BGAN will employ terminals with omnidirectional antennas. It will be easier to set up, will require less complex maintenance, and will function in aeronautical and marine environments as well as from fixed dry-land surface points.

1.2.7 Space network

Space Network is a NASA program that combines space and ground elements to support spacecraft communications in Earth vicinity. The SN Project Office at Goddard Space Flight Center manages the SN. Space networks are networks used for communication between spacecraft, usually in the vicinity of the Earth. The example of this is NASA's Space Network.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. II, Issue IV, April 2016.

1.3 CHARACTERISTICS OF WIRELESS NETWORKS

1.3.1 Node deployment

Node deployment in WSNs is application dependent and affects the performance of the routing protocol. The deployment can be either deterministic or randomized. In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths. However, in random node deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner. If the resultant distribution of nodes is not uniform, optimal clustering becomes necessary to allow connectivity and enable energy efficient network operation. Inter sensor communication is normally within short transmission ranges due to energy and bandwidth limitations. Therefore, it is most likely that a route will consist of multiple wireless hops.

1.3.2 Energy consumption without losing accuracy

Sensor nodes can use up their limited supply of energy performing computations and transmitting information in a wireless environment. As such, energy- conserving forms of communication and computation are essential. Sensor node lifetime shows a strong dependence on the battery lifetime. In a Multi-hop WSN, each node plays a dual role as data sender and data router. The malfunctioning of some sensor nodes due to power failure can cause significant topological changes and might require rerouting of packets and reorganization of the network.

1.2.3 Fault Tolerance

Some sensor nodes may fail or be blocked due to lack of power, physical damage, or environmental interference. The failure of sensor nodes should not ffect the overall task of the sensor network. If many nodes fail, MAC and routing protocols must accommodate formation of new links and routes to the data collection base stations. This may require actively adjusting transmit powers and signaling rates on the existing links to reduce energy consumption, or rerouting packets through regions of the network where more energy is available. Therefore, multiple levels of redundancy may be needed in a fault-tolerant sensor network.

1.3.4 Scalability

The number of sensor nodes deployed in the sensing area may be in the order of hundreds or thousands, or more. Any routing scheme must be able to work with this huge number of sensor nodes. In addition, sensor network routing protocols should be scalable enough to respond to events in the environment. Until an event occurs, most of the sensors can remain in the sleep state, with data from the few remaining sensors providing a coarse quality.

1.3.5 Node/Link Heterogeneity

In many studies, all sensor nodes were assumed to be homogeneous, i.e., having equal capacity in terms of computation, communication, and power. However, depending on the application a sensor node can have different role or capability. The existence of heterogeneous set of sensors raises many technical issues related to data routing. For example, some applications might require a diverse mixture of sensors for monitoring temperature, pressure and humidity of the surrounding environment, detecting motion via acoustic signatures, and capturing the image or video tracking of moving objects. These special sensors can

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. II, Issue IV, April 2016.

be either deployed independently or the different functionalities can be included in the same sensor nodes.

1.4 CHALLENGES AND DESIGN ISSUES IN WIRELESS NETWORKS

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes.Wireless networking is a method by which homes, telecommunications networks and enterprise installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless networks are computer networks that are not connected by cables of any kind. The use of a wireless network enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations. The basis of wireless systems are radio waves, an implementation that takes place at the physical level of network structure[1].

1.4.1 Resource constraints

The design and implementation ofWSNs are constrained by three types of resources: a) energy; b) memory; and c) processing. Constrained by the limited physical size, sensor nodes have limited battery energy supply.At the same time, their memories are limited and have restricted computational capabilities.

1.4.2 Dynamic topologies and harsh environmental conditions

In industrial environments, the topology and connectivity of the network may vary due to link and sensor-node failures. Furthermore, sensors may also be subject to RF interference, highly caustic or corrosive environments, high humidity levels, vibrations, dirt and dust, or other conditions that challenge performance.These harsh environmental conditions and dynamic network topologies may cause a portion of industrial sensor nodes to malfunction.

1.4.3 Quality-of-service requirements

The wide variety of applications envisaged on IWSNs will have different QoS requirements and specifications. The QoS provided by IWSNs refers to the accuracy between the data reported to the sink node and what is actually occurring in the industrial environment. In addition, since sensor data are typically time-sensitive, e.g., alarm notifications for the industrial facilities, it is important to receive the data at the sink in a timely manner. Data with long latency due to processing or communication may be outdated and lead to wrong decisions in the monitoring system[11].

1.4.4 Data redundancy

Because of the high density in the network topology, sensor observations are highly correlated in the space domain. In addition, the nature of the physical phenomenon constitutes the temporal correlation between each consecutive observation of the sensor node.

1.4.5 Packet errors and variable-link capacity

Compared to wired networks, in IWSNs, the attainable capacity of each wireless link depends on the interference level perceived at the receiver, and high bit error rates are observed in communication. In addition, wireless links exhibit widely

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. II, Issue IV, April 2016.

varying characteristics over time and space due to obstructions and noisy environment.

1.4.6 Security

Security should be an essential feature in the design of IWSNs to make the communication safe from external denial-of-service attacks and intrusion. IWSNs have special characteristics that enable new ways of security attacks. Passive attacks are carried out by eavesdropping on transmissions including traffic analysis or disclosure of message contents. Active attacks consist of modification, fabrication, and interruption, which in IWSN cases may include node capturing, routing attacks, or flooding[9].

1.4.7 Large-scale deployment and ad hoc architecture

Most IWSNs contain a large number of sensor nodes hundreds to thousands or even more, which might be spread randomly over the deployment field. Moreover, the lack of predetermined network infrastructure necessitates the IWSNs to establish connections and maintain network connectivity autonomously.

1.4.8 Integration with Internet and other networks

It is of fundamental importance for the commercial development of IWSNs to provide services that allow the querying of the network to retrieve useful information from anywhere and at any time. For this reason, the IWSNs should be remotely accessible from the Internet and, hence, need to be integrated with the Internet Protocol architecture.

1.5 FEATURES OF WIRELESS NETWORKS

Current technological innovations have turned us towards a strong reliance on our beloved mobile devices.

1.5.1 High Capacity Load Balancing

Wireless networks were originally planned for coverage only, but with all the smartphones, tablets, e-readers, etc. out there, today's wireless networks must be planned for capacity. With the increased demand on the wireless network infrastructure, you must incorporate high capacity load balancing. This means, when one access point is overloaded, this allows the system to actively shift users from one AP to another depending on the capacity that is available.

1.5.2 Scalability

The growth in popularity of new wireless gadgets has will only continue to grow. Your network needs to have the ability to start small if necessary, but expand in terms of coverage and capacity as needed without having to overhaul or build an entirely new network. Trust me, if you don't need it now, you will need it later.

1.5.3 Centralized Management

Modern day wireless networks are much more complex and may consist of hundreds or even thousands of access points. Therefore, you will require a smarter way of managing all the access points within your network, namely, centralized management. Updates and configuration changes should be made once and the system updates all access points across your network.

1.5.4 Role Based Access Control

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. II, Issue IV, April 2016.

Role based access control allows you to assign a role to the wireless device based on how it authenticated. Your wireless network system should integrate with the active directory and assign a role based on who are. Once the role of the device is defined, access control rules can be applied to it. You can segment users into groups to limit what can access based on their role.

1.5.5 Indoor as well as Outdoor coverage options

Although you may only feel you need indoor coverage at first, you will probably later be adding outdoor coverage to parking lots, courtyards, etc. Therefore, in your wireless network system, there needs to be an easy way to add indoor and outdoor coverage all from the same platform.

1.5.6 Real Time Wireless Visibility

For all wireless networks, you need to have the ability to see the user in real time, what type of device there are using, what type of coverage shows in that area, and the status of the different networking component s that may affect the use of that device. Your IT staff needs to be able to see what's going on in order to address any issues.

1.5.7 Device Registration Network Access Control

Whether you refer to it as mobile device registration or network access control, it is essential to have a secure method for registering devices that you don't own. Primarily, NAC controls the role of the user and enforces policies. Network access control can allow the users to register themselves to the network. You must also be able to enforce policies by checking for things like the latest updates or if have anti-virus, etc. This will save your IT a lot of headache.

1.5.8 Ability to communicate with both 2.4 GHz devices and 5 GHz devices

Baby scanners, blue tooth, microwaves, and many of today's common use devices can interfere with users on 2.4 GHz devices- simply put it's a "crowded spectrum". Since many devices still operate in that spectrum, you'll need dual radio access points that can manage users on both 2.4 GHz and 5 GHz at the same time.

1.5.9 Web Content/Application Filtering

More than ever before, network security must become application aware in order to alleviate application threats. You should have application filtering in place in order to protect users from bad content and prevent performance issues.

1.5.10 Mobile Device Management

Think about all those mobile device that will be accessing your wireless network; now think about the thousands of applications you're going to have running on your wireless network on those mobile devices. You obviously need a way to manage this. Mobile device management can provide control of how you will manage access to applications and programs.Even remotely wipe the device if it's lost or stolen.

1.5.11 Quality of Service/Application Prioritization

Quality of service simply means that you should be able to determine what uses are most important to take priority over someone streaming Netflix.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. II, Issue IV, April 2016.

1.6 ROUTING IN WIRELESS NETWORKS

Routing is the process of selecting best paths in a network. In the past, the term routing also meant forwarding network traffic among networks. However, that latter function is better described as forwarding. Routing is performed for many kinds of networks, including the telephone network, electronic data networks such as theInternet, and transportation networks. This article is concerned primarily with routing in electronic data networks using packet switching technology.

In packet switching networks, routing directs packet forwarding the transit of logically addressed network packets from their source toward their ultimate destination through intermediate nodes. Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, firewalls, or switches. General-purpose computers can also forward packets and perform routing, though are not specialized hardware and may suffer from limited performance.

The routing process usually directs forwarding on the basis of routing tables, which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing. Most routing algorithms use only one network path at a time. Multipath routing techniques enable the use of multiple alternative paths.

In case of overlapping/equal routes, algorithms consider the following elements to decide which routes to install into the routing table :

1. Prefix-Length: where longer subnet masks are preferred independent of whether it is within a routing protocol or over different routing protocol.
2. Metric: where a lower metric/cost is preferred only valid within one and the same routing protocol.
3. Administrative distance: where a route learned from a more reliable routing protocol is preferred only valid between different routing protocols.

Routing, in a more narrow sense of the term, is often contrasted with bridging in its assumption that network addresses are structured and that similar addresses imply proximity within the network. Structured addresses allow a single routing table entry to represent the route to a group of devices. In large networks, structured addressing routing, in the narrow sense outperforms unstructured addressing . Routing has become the dominant form of addressing on the Internet. Bridging is still widely used within localized environments.

1.7 ROUTING SCHEMES IN WIRELESS NETWORKS

1.7.1 unicast

Unicast is the dominant form of message delivery on the Internet. This article focuses on unicast routing algorithms.The term unicast is contrasted with the term broadcast which means transmitting the same data to all possible destinations. Another multi-destination distribution method, multicasting, sends data only to interested destinations by using special address assignments.If an IP Unicast packet passes through a switch that does not know the location of the associated MAC Address, the packet will be broadcast to all ports on the switch. This failure of Unicast to 'cast to a single

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. II, Issue IV, April 2016.

device' is called a Unicast flood.Unicast messaging is used for all network processes in which a private or unique resource is requested.Certain network applications which are mass-distributed are too costly to be conducted with unicast transmission since each network connection consumes computing resources on the sending host and requires its own separate network bandwidth for transmission. Such applications include streaming media of many forms. Internet radio stations using unicast connections may have high bandwidth costs.

1.7.2 broadcasting

In computer networking, broadcasting refers to transmitting a packet that will be received by every device on the network. In practice, the scope of the broadcast is limited to a broadcast domain. Broadcast a message is in contrast to unicast addressing in which a host sends datagrams to another single host identified by a unique IP address.Broadcasting is the most general communication method, and is also the most intensive in the sense that a large number of messages are required.Broadcasting may be performed as all scatter in which each sender performs its own scatter in which the messages are distinct for each receiver, or all broadcast in which are the same.The MPI message passing method which is the de facto standard on large computer clusters includes the MPI_Alltoall method.Not all network technologies support broadcast addressing; for example, neither X.25 nor frame relay have broadcast capability, nor is there any form of Internet-wide broadcast. Broadcasting is largely confined to local area network technologies, most notably Ethernet and token ring, where the performance impact of broadcasting is not as large as it would be in a wide area network.The successor to Internet Protocol Version 4 , IPv6 also does not implement the broadcast method, so as to prevent disturbing all nodes in a network when only a few may be interested in a particular service.

Instead it relies on multicast addressing - a conceptually similar one-to-many routing methodology. However, multicasting limits the pool of receivers to those that join a specific multicast receiver group.Both Ethernet and IPv4 use an all-ones broadcast address to indicate a broadcast packet. Token Ring uses a special value in the IEEE 802.2 control field.Broadcasting may be abused to perform a type of DoS-attack known as a Smurf attack. The attacker sends fake ping requests with the source IP-address of the victim computer. The victim computer is flooded by the replies from all computers in the domain.These terms are also used by streaming content providers' services. Unicast-based media servers open and provide a stream for each unique user. Multicast-based servers can support a larger audience by serving content simultaneously to multiple users.

1.7.3 multicast

In computer networking, multicast one-to-many or many-to-many distributionis group communication where information is addressed to a group of destination computers simultaneously. Multicast should not be confused with physical layer point-to-multipoint communication.Group communication may either be application layer multicast or network assisted multicast, where the latter makes it possible for the source to efficiently send to the group in a single transmission.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. II, Issue IV, April 2016.

Copies are automatically created in other network elements, such as routers, switches and cellular network base stations, but only to network segments that currently contain members of the group.

Network assisted multicast may be implemented at the Internet layer using IP multicast, which is often employed in Internet Protocol applications of streaming media, such as Internet television scheduled content but not media-on-demand and multipoint videoconferencing, but also for ghost distribution of backup disk images to multiple computers simultaneously. In IP multicast the implementation of the multicast concept occurs at the IP routing level, where routers create optimal distribution paths for datagrams sent to a multicast destination address.Network assisted multicast may also be implemented at the Data Link Layer using one-to-many addressing and switching such as Ethernet multicast addressing, Asynchronous Transfer Mode point-to-multipoint virtual circuits or Infiniband multicast.

1.7.4 anycast

On the Internet, anycast is usually implemented by using Border Gateway Protocol to simultaneously announce the same destination IP address range from many different places on the Internet. This results in packets addressed to destination addresses in this range being routed to the nearest point on the net announcing the given destination IP address. In the past, anycast was suited to connectionless protocols generally built on UDP, rather thanconnection-oriented protocols such as TCP that keep their own state. However, assuming a deterministic destination selection for all packets within a session, TCP does work with anycasted destinations. With TCP anycast, there are cases where the receiver selected for any given source may change from time to time as optimal routes change, silently breaking any conversations that may be in progress at the time. These conditions are typically referred to as a pop switch. To correct this issue, there have been proprietary advancements within custom IP stacks which allow for healing of stateful protocols where it is required. For this reason, anycast is generally used as a way to provide high availability and load balancing for stateless services such as access to replicated data; for example, DNS service is a distributed service over multiple geographically dispersed servers.

1.7.5 Geocast

Geocast refers to the delivery of information to a group of destinations in a network identified by their geographical locations. It is a specialized form of multicast addressing used by some routing protocols for mobile ad hoc networks.

2 PERFORMANCE ANALYSIS

To analysis the performance of the proposed method, several performance metrics are used. These are Packet Delivery Ratio, Route Lifetime Analysis.

2.1 Packet Delivery Ratio

Packet Delivery Ratio is calculated as the tradeoff between the number of packet by packet sending time.

$$\text{PACKET DELIVERY RATIO} = \frac{\text{NUMBER OF PACKETS}}{\text{TIME}}$$

CONCLUSION

Thus the E-STAR uses payment/trust systems with trust-based and energy-aware routing protocol to establish

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. II, Issue IV, April 2016.

stable/reliable routes in HMWNs. The E-STAR stimulates the nodes not only to relay others' packets but also to maintain the route stability. The proposed SRR and BAR routing protocols and evaluated them in terms of overhead and route stability. The protocols can make informed routing decisions by considering multiple factors, including the route length, the route reliability based on the nodes' past behavior, and the route lifetime based on the nodes' energy capability. SRR establishes routes that can meet source nodes' trust/energy requirements. It is useful in establishing routes that avoid the low-trust nodes, e.g., malicious nodes, with low overhead. For BAR, destination nodes establish the most reliable routes but with more overhead comparing to SRR. The analytical results have demonstrated that E-STAR can secure the payment and trust calculation without false accusations.

REFERENCES

1 G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J., vol. 13, no. 4, pp. 175-193, 2009.

2 C. Chou, D. Wei, C. Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, Jan. 2007.

2 S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom'00, pp. 255-265, Aug. 2000.

3 X. Li, Z. Li, M. Stojmenovic, V. Narasimhan, and A. Nayak, "Autoregressive Trust Management in Wireless Ad Hoc Networks," Ad Hoc & Sensor Wireless Networks, vol. 16, no. 1-3 , pp. 229-242, 2012.

4 G. Indirania and K. Selvakumara, "A Swarm-Based Efficient Distributed Intrusion Detection System for Mobile Ad Hoc Networks (MANET)," Int'l J. Parallel, Emergent and Distributed Systems, vol. 29, pp. 90-103, 2014.

5 H. Li and M. Singhal, "Trust Management in Distributed Systems," Computer, vol. 40, no. 2, pp. 45-53, Feb. 2007.

6 K. Liu, J. Deng, and K. Balakrishnan, "An AcknowledgementBased Approach for the Detection of Routing Misbehavior in MANETs," IEEE Trans. Mobile Computing, vol. 6, no. 5, pp. 536550, May 2007.

7 S. Zhong, J. Chen, and R. Yang, "Sprite: A Simple, Cheat-Proof, Credit Based System for Mobile Ad-Hoc Networks," Proc. IEEE INFOCOM '03, vol. 3, pp. 1987-1997, Mar./Apr. 2003.

8 M. Mahmoud and X. Shen, "PIS: A Practical Incentive System For Multi-Hop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 59, no. 8, pp. 4012-4025, Oct. 2010.

9 M. Mahmoud and X. Shen, "ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-Hop Wireless Networks," IEEE Trans. Mobile Computing, vol. 10, no. 7, pp. 9971010, July 2011.

10 M. Mahmoud and X. Shen, "An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Drop in Multihop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 60, no. 8, pp. 3947-3962, Oct. 2011.

11 G. Theodorakopoulos and J.S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 318-328, Feb. 2006.

12 P. Velloso, R. Laufer, D. Cunha, O. Duarte, and G. Pujolle, "Trust Management in Mobile Ad Hoc

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. II, Issue IV, April 2016.

Networks Using a Scalable Maturity-Based Model," IEEE Trans. Network and Service Management, vol. 7, no. 3, pp. 172-185, Sept. 2010.

13 S. Lindsay, Y. Wei, H. Zhu, and K. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 305317, Feb. 2006.

14 M. Yu and K. Leung, "A Trustworthiness-Based QoS Routing Protocol for Wireless Ad Hoc Networks," IEEE Trans. Wireless Comm., vol. 8, no. 4, pp. 1888-1898, Apr. 2009.

15 D. Johnson, D. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks," Ad Hoc Networking, C. Perkins, ed., chapter 5, pp. 139-172, AddisonWesley, 2001.