www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 3 March 2015, Page No. 10690-10696

Improving the Hybrid Ad hoc Network Routing Performance Using RMECR Algorithm and Lightweight protocol

R Priya, H Prabavathi
M.E., Department of Computer Science and engineering,
A.V.C. College of Engineering,
Mayiladuthurai, Tamil Nadu, India.
ramadurai.priya@gmail.com
Assistant Professor, Department of Computer Science and Engineering,
A.V.C. College of Engineering,
Mayiladuthurai, Tamil Nadu, India.
prabavathih@gmail.com

Abstract-The work deals with the problem of energy-efficient reliable wireless communication in the presence of unreliable or loss wireless link layers in multi-hop wireless networks. RMER and RMECR are proposed for networks in which either hop-by-hop or end-to-end retransmissions ensure reliability. Simulation studies show that RMECR is able to find energy-efficient and reliable routes similar to RMER while also extending the operational lifetime of the network. This makes RMECR an elegant solution to increase energy efficiency, reliability and lifetime of wireless ad hoc networks. We conducted extensive simulations to study the power consumption, the end-to-end delay and the network throughput of our protocols compared with the existing protocols. In contrast to the conventional power-aware algorithms, the Maximum Residual Packet Capacity (MRPC) identifies the capacity of a node not just by its residual battery energy but also by the expected energy spent in reliably forwarding a packet over a specific link. In this paper we argue that such a formulation based solely on the energy spent in single transmission is misleading —the proper metric should include the total energy (including that expended for any retransmissions necessary) spent in reliably delivering the packet to its final destination. In focus of achieving secure communication and preserving user's privacy in hybrid ad hoc wireless networks, to preserve user's anonymity each node uses pseudonyms and one-time session key. In addition to secure the communication, this paper develops efficient pseudonym generation and trapdoor techniques require only lightweight hashing operations and a payment system.

Index terms- Hybrid ad-hoc networks, anonymous, energy-aware routing, end-to-end and hop-by-hop retransmission.

1 INTRODUCTION

"Ad Hoc" is actually a Latin phrase that means "for this purpose." It is often used to describe solutions that are developed on-the-fly for a specific purpose. In computer networking, an ad hoc network refers to a network connection established for a single session and does not require a router or a wireless base station. For example, if you need to transfer a file to your friend's laptop, you might create an ad hoc network between your computer and his laptop to transfer the file. This may be done using an Ethernet crossover cable, or the computer's wireless cards to communicate with each other. If you need to share files with more than one computer, you could set up a multi-hop ad hoc network, which can transfer data over multiple nodes. Basically, an ad hoc network is a temporary network connection created for a specific purpose (such as transferring data from one computer to another). If the network is set up for a longer period of time, it is just a plain old local area network (LAN).

2 RELATED WORKS

The energy-aware routing algorithms for wireless ad hoc networks, called Reliable Minimum Energy Cost Routing (RMECR) and Reliable Minimum Energy Routing (RMER). RMECR addresses three important requirements of ad hoc networks: energy-efficiency, reliability and prolonging network lifetime. It considers the energy consumption and the remaining battery energy of nodes as well as quality of links to find energy-efficient and reliable routes that increase the operational lifetime of the network. RMER on the other hand is an energy-efficient routing algorithm which finds routes minimizing the total energy required for end-to-end packet traversal. RMER and RMECR are proposed for networks in which either Hop-by-Hop or end-to-end retransmissions ensure reliability. Simulation studies show that RMECR is able to find energy-efficient and reliable routes similar to RMER while also extending the operational lifetime of the network. This makes RMECR an elegant solution to increase energy-efficiency, reliability and lifetime of wireless ad hoc networks. In the design of RMECR consider minute details such as energy consumed by processing elements of transceivers, limited number of retransmissions allowed per packet, packet sizes and the impact of acknowledgment packets. This adds the novelty of this work compared to the existing studies. Secure communication and preserving user's privacy in hybrid ad hoc wireless networks. To preserve user's anonymity each node uses pseudonyms and one-time session key. This paper develops efficient pseudonym generation and trapdoor techniques require only lightweight hashing operations and a payment system.

3 SYSTEM MODELS

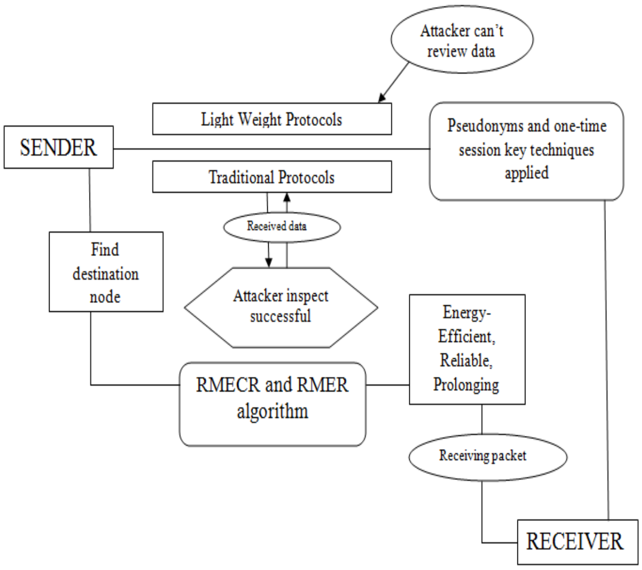
Attacker can't review data
Light Weight Protocols
SENDER
Pseudonyms and one-time session key techniques applied
Traditional Protocols
Received data
Find destination node
Attacker inspect successful
Energy-Efficient, Reliable, Prolonging
RMECR and RMER algorithm
Receiving packet
RECEIVER

Fig.1. Architecture

4 THE PROPOSED PROTOCOL

4.1 Nodes Information Gathering and Reliable Route Identification

The represented topology of a wireless ad hoc networks by a graph; IEÞ, where VV and IE are the set of nodes (vertices) and links (edges) respectively. Each node is assigned a unique integer identifier between 1 and *n*. Nodes are assumed to be battery powered. The remaining battery energy of node *u* to VV is represented by node if the battery energy of a node all below a threshold value, the node is considered to be dead. Without loss of generality we assume C0. A link in the network is denoted in which *u* and *v* are sending and receiving nodes respectively. The criterion for having a link from *u* to *v* is as follows: There could be a link from *u* to *v*, if the received signal strength by *v* is above a threshold. This threshold is usually specified in such a way that a targeted link error probability is satisfied. We denote the probability of error-free reception of packets of length *x* [bit] transmitted by *u* to *v*. In other words is the packet delivery ratio of for packets of size *x*.

As an essential requirement for energy-efficient routing we assume nodes support adjustable transmission power. The transmission power from node *u* to node *v* is denoted by a finite set of allowable transmission powers for node *u* specified by S, where *u* is the number of allowable transmission powers of node *u*. The discrete set is due to the practical considerations that all the commercially available devices are preprogrammed with a set of power settings. Regarding the power adjustment by nodes, we assume:

1) P is the minimum transmission power from S that satisfies the targeted link error probability.

2) By adjusting the transmission power, the data rate of the physical link does not change. We represent a path in the network with h hops between two nodes as a set of node where *n2* is the identifier of the *k* the node of the path. Here, *n1* is the source node, *nh1* is the destination node, and the rest are intermediate nodes which relay packets from the source to the destination hop by hop. Furthermore IE is the link of the path.

4.2 Routing and Prolonging Network Lifetime

Reliability and energy cost of routes must be considered in route selection. The key point is that energy cost of a route is related to its reliability. If routes are less reliable, the probability of packet retransmission increases. Thus, a larger amount of energy will be consumed per packet due to retransmissions of the packet. By defining two different ways of computing the energy cost of routes we design two sets of energy-aware reliable routing algorithms for hop-by-hop and end-to-end systems. They are called Reliable Minimum Energy Cost Routing (RMECR) and Reliable Minimum Energy Routing (RMER). In RMER, energy cost of a path for end-to-end packet traversal is the expected amount of energy consumed by all nodes to transfer the packet to the destination. In RMECR, the energy cost of a path is the expected battery cost of nodes along the path to transfer a packet from the source to the destination. Before we proceed with the design of RMER and RMECR we first define Minimum Energy Cost Path.

Energy-aware routing algorithms for wireless ad hoc networks called Reliable Minimum Energy Cost Routing (RMECR) and Reliable Minimum Energy Routing (RMER). RMECR addresses three important requirements of ad hoc networks: energy-efficiency, reliability and prolonging network lifetime. It considers the energy consumption and the remaining battery energy of nodes as well as quality of links to find energy-efficient and reliable routes that increase the operational lifetime of the network. RMER on the other hand is an energy-efficient routing algorithm which finds routes minimizing the total energy required for end-to-end packet traversal. RMER and RMECR are proposed for networks in which either Hop-by-Hop or end-to-end retransmissions ensure reliability. Simulation studies show that RMECR is able to find energy-efficient and reliable routes similar to RMER while extending the operational lifetime of the network.

4.3 Authentication and Pseudonym Generation Technique

Developing low-overhead secure and privacy-preserving communication protocol is a real challenge due to the inherent contradictions. First, securing the protocol usually requires each node to use one authenticated identity but a permanent identity should not be used to preserve the node's privacy. Second, reducing the protocol's overhead is necessary because the nodes are constrained by limited battery energy and computing power. However, the low overhead requirement contradicts with the large overhead usually needed for preserving privacy and securing the communication. Our protocol enables the nodes to establish routes and send/relay packets without revealing their real identities or the identity of the destination node. A node's pseudonyms can authenticate it to the intended nodes without revealing its real identity. Packet tracing is prevented by changing the packet's appearance (bits) at each hop and using packet mixers. Therefore, even if an attacker eavesdrops on both the source and destination nodes, he/she cannot correlate their packets. To secure the protocol and preserve privacy the intermediate nodes can ensure that the packets are sent by legitimate nodes without revealing the real identities of the source and destination nodes. The server only lets a remote user log in if that user can prove that they have the right to access that account. Depending on the server's configuration and the user's choice, the user may present one of several forms of credentials. The user may present the password for the account that he is trying to log into; the server then verifies that the password is correct. The user may present a public key and prove that she/he possesses the private key associated with that public key. This is exactly the same method that is used to authenticate the server but now the user is trying to prove its identity and the server is verifying it. The login attempt is accepted if the user proves that she/he knows the private key and the public key is in the account's authorization.Another type of method involves delegating part of the work of authenticating the user to the client machine. This happens in controlled environments such as enterprises, when many machines share the same accounts.

The server authenticates the client machine by the same mechanism that is used the other way round and then relies on the client to authenticate the user. Long-term identity or a permanent group of pseudonyms can violate user’s privacy. Attackers can link the identity or the pseudonyms to the user, e.g., by analyzing the associated activities. To preserve user’s anonymity, each pseudonym is used for short time in such a way that only the intended node can link the pseudonyms to each other. By this way, even if an attacker could link a pseudonym to the user in one occasion, she/he cannot violate the user’s privacy for a long time and will not benefit from this conclusion in the future due to pseudonym’s periodic change and unlikability. Using a pseudonym for a long time enables attackers to collect much information about the visited locations by the anonymous user. Then, by analyzing this information the attackers may identify the users and gain much information about their past visited locations. The requirement that a node should not change its pseudonym more than once before the other node changes its pseudonym, can work well if the two nodes exchange packets regularly. However, in some cases such as route request packets a node may send multiple packets before receiving a packet from the other node.

This requirement can be relaxed if each node matches the other node’s pseudonym against a window of ‘L’ expected pseudonyms, the node should advance the window when it receives a pseudonym, where the last released pseudonym is always on top of the window. Each node can release up to L pseudonyms before receiving a packet from the other node without losing synchronization. Since privacy is a user-specific concept, our pseudonym generation technique allows users to trade off the privacy level and the computational overhead. Pseudonym change can be arbitrarily triggered by any of the two nodes without losing synchronization. The frequency of pseudonym change *Fr* is the number of packets that use one pseudonym. Higher privacy level is obtained when *Fr* decreases. The highest privacy level can be obtained when *Fr=1*, i.e., a pseudonym is used for only one packet. Another advantage in our technique is that pseudonyms are computed by lightweight hashing operations and do not require large storage area or pseudonym refilling (unlike). This means that *Fr* can be few (to boost node’s privacy) with an acceptable overhead. Pseudonyms can also be computed before receiving a packet to avoid delaying the packet relay..

4.4 Secure Data Process

It stores each route’s pseudonyms and keys in memory, so that it can quickly verify whether a packet is targeted at it or not and which pseudonym/key it has to use. Each intermediate node replaces the incoming pseudonym with the outgoing one shared with the next node, and encrypts the iteratively-encrypted part with the key shared with base station. Thus, when the packet reaches the source base station, it should have a layered-encrypted cipher text that is computed by all the nodes in the uplink route. The source base station removes the encryption layers by iteratively decrypting the packet with the keys shared with the nodes in the route. It also verifies the attached hash value to make sure that the message has not been modified during transmission. If this verification fails, the base station sends a negative acknowledgement to the source node to retransmit the message, otherwise, it forwards the message to the destination base station if the destination node resides in a different cell the destination base station iteratively encrypts the message with the keys shared with the nodes in the route and sends the packet to the first node in the route. Each intermediate node removes one encryption layer and replaces the pseudonym with the one shared with the next node.

The destination node decrypts the packet and verifies the hash value to ensure the message's integrity and authenticity. For reliable communication, the destination node sends back an acknowledgement packet when it receives a correct message. Note that the session keys are used only for generating one-time pseudonyms but the keys shared with the base station are used in encryption to prevent manipulating the messages and secure the payment by thwarting free riding attack. Moreover, the time element in *Uni* can guarantee that the packets look different if the same message is sent at different times this can protect the node's anonymity against fingerprint recording attack. To reduce the overhead on the mobile nodes, each node performs one encryption/decryption operation but the base station performs more operations. To simplify our description, we focus on unidirectional data transmission but the protocol can also be used for bidirectional communication. A route is broken when two neighboring nodes in the route cannot communicate, e.g., because they are no longer in transmission range due to node mobility. When a node forwards a packet to its neighbor, it can confirm that the neighbor received the packet by link-layer acknowledgment.

A route is considered broken if a node does not receive an acknowledgment after a limited number of packet retransmissions. In this case, the node should send an error packet to the base station to re-establish the route. Moreover, the base station can determine route breakage by re-starting a timer each time it receives a data or acknowledgement packet, and the route is considered broken if the timer expires. To reduce the overhead of reconnecting the broken routes, the base station can cache the routing information when it receives route discovery packets and uses this information when it needs to establish a route by unicasting a DREST packet.

4.5 Authentication key and Route Module

Uplink route between (NS) source node's base station (Bs) and Downlink route between (ND) destination node's base station (Bd). To establish end-to-end route, NS broadcasts the Uplink Route Request Packet (URREQ) and Bs forwards a call request to the destination node's base station if ND resides in a different cell. Bd broadcasts Destination Notification Packet (DNOT) if it does not know a route to ND to inform the node about the call request. ND replies with Downlink Route Request Packet (DRREQ) to enable Bd to know the identities of the intermediate nodes in the route. Finally, Bs and Bd send Uplink Route Establishment Packet (UREST) and Downlink Route Establishment Packet (DREST), respectively to establish the route. The source node initiates route discovery by broadcasting URREQ packet containing a unique request identifier(*Uni*), time to live (TTL) and the encryption of *Uni*, the source and the destination node's real identities, dummy bits called padding (Pad) and the padding length. *Uni* is the pseudonym shared and time stamp. Each node and the base station process only the first received URREQ packet and discard all further packets having the identifier *Uni*. Using this identifier is necessary to avoid routing loops and broadcast Authentication phase packets. Explosion that causes broadcasting the same packet each time it is received from a neighbor. This identifier does not reveal much information because the packets are broadcasted. *IDSBs* and the encrypted part authenticate NS to Bs, which is necessary for authorizing the network access and securing the payment.

TTL is used to bind the request propagation area. Each node decrements TTL, and once it is zero the request is no longer broadcasted. Each node adds the pseudonym shared with Bs, encrypts the previous node's pseudonym and the encrypted part with the shared key with Bs, and broadcasts b the request. As the packet moves towards the base station, it stores the pseudonyms of the nodes in the route. For the first received URREQ packet, Bs decrypts the encryption layers to tell the identities of the source, intermediate, and destination nodes. Then, it sends call request to Bd if ND resides in a different cell. Since the packet length grows with fixed amount of data as it is relayed, the attackers may try to locate the source node's location either from TTL or the packet size. To protect the location privacy of NS and to confuse its neighbors whether the packet is originated from or relayed by NS, random-length padding is added and the initial TTL is variable value. Since Uni varies over time, each time a node sends URREQ packet to the same destination, the packet looks different in spite of using the same key.

5 PERFORMANCE EVALUATION

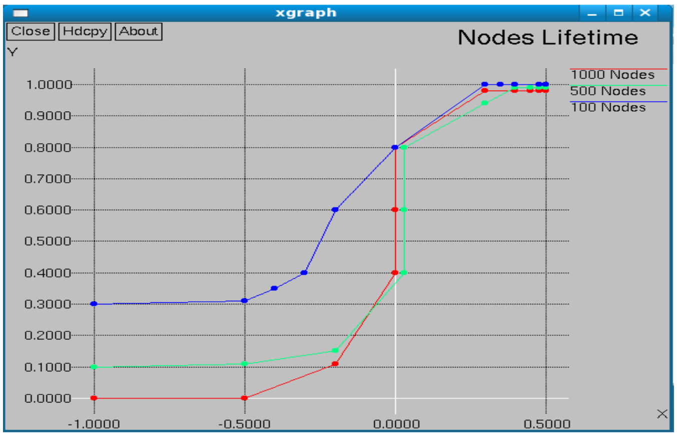

Fig.2.Nodes Lifetime

6 CONCLUSION

An in-depth study of energy-aware routing in ad hoc networks is presented and a new routing algorithm for wireless ad hoc networks via, Reliable Minimum Energy Cost Routing (RMECR) is proposed. RMECR can increase the operational lifetime of the network using energy-efficient and reliable routes. In the design of RMECR the detailed energy consumption model for packet transfers in wireless ad hoc networks. RMECR was designed for two types of networks: those in which Hop-by-Hop retransmissions ensure reliability and those in which end-to end retransmissions ensure reliability. The general approach that used in the design of RMECR was used to also devise a state-of-the-art energy-efficient routing algorithm for wireless ad hoc networks, i.e., Reliable Minimum Energy Routing (RMER). RMER finds routes minimizing the energy consumed for packet traversal. RMER does not consider the remaining battery energy of nodes and was used as a benchmark to study the energy-efficiency of the RMECR algorithm. Extensive simulations showed that RMER not only saves more energy compared to existing energy efficient routing algorithms, but also increases the reliability of wireless ad hoc networks. Furthermore it is observed that RMECR finds routes that their energy efficiency and reliability are almost similar to that of routes discovered by RMER. However, RMECR also extends the network lifetime by directing the traffic to nodes having more amount of battery energy. We propose a lightweight secure communication and privacy preserving protocol for hybrid ad hoc network. To reduce the overhead the light weight protocol, pseudonyms techniques and one-time session key is used. The proposed algorithms are implemented on a test bed to study the impact of varying conditions on the performance of all those techniques.

REFERENCES

[1] Vazifehdan, Javad, R. Venkatesha Prasad, and Ignas Niemegeers. "Energy-efficient reliable routing considering residual energy in wireless ad hoc networks." *IEEE Transactions on Mobile Computing* 2 (2014): 434-447.

[2] Mahmoud, Mohamed MEA, et al. "Lightweight privacy-preserving and secure communication protocol for hybrid ad hoc wireless networks." *Parallel and Distributed Systems, IEEE Transactions on* 25.8 (2014): 2077-2090.

[3] Banerjee, Suman, and Archan Misra. "Minimum energy paths for reliable communication in multi-hop wireless networks." *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*. ACM, 2002.

[4] Li, XiangYang, et al. "Energy efficient routing with unreliable links in wireless networks." *Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on*. IEEE, 2006.

[5] Misra, Archan, and Suman Banerjee. "MRPC: Maximizing network lifetime for reliable routing in wireless environments." *Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE*. Vol. 2. IEEE, 2002.

[6] Gomez, Javier, et al. "PARO: supporting dynamic power controlled routing in wireless ad hoc networks." *Wireless Networks* 9.5 (2003): 443-460.

[7] Upadhyaya, S., et al. "Minimum Cost Blocking Problem in Multi-path Wireless Routing Protocols." (2013): 1-1.

[8] Mahmoud, Mohamed Elsalih, and Xuemin Shen. "Lightweight privacy-preserving routing and incentive protocol for hybrid ad hoc wireless network."*Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on*. IEEE, 2011.

[9] Ben Salem, Naouel, et al. "Node cooperation in hybrid ad hoc networks."*Mobile Computing, IEEE Transactions on* 5.4 (2006): 365-376.

[10] Mahmoud, Mohamed Elsalih, and Xuemin Shen. "Esip: secure incentive protocol with limited use of public-key cryptography for multihop wireless networks." *Mobile Computing, IEEE Transactions on* 10.7 (2011): 997-1010.

[11] Mahmoud, Mohamed Elsalih, and Xuemin Shen. "Stimulating cooperation in multi-hop wireless networks using cheating detection system." *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010.