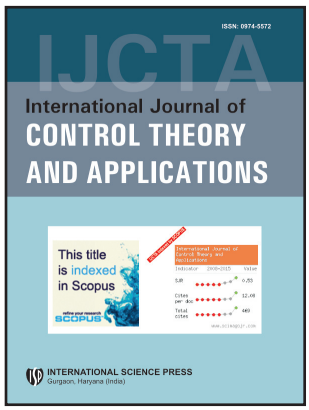

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 16 • 2017

A Review of Routing Protocols in Hybrid Networks

R. Arun[a] and V. Jeyalakshmi[b]

[a]*Research Scholar, St.Peter's University, Chennai, India. Email: arun_ece05@yahoo.co.in*
[b]*Professor, Anna University, Chennai, India. Email: jpjeya@gmail.com*

Abstract: This paper evaluates and compare Mobile Ad hoc Network (MANET) routing protocols for Wireless Sensor Networks (WSNs). It aims and compares the performance based on Quality of service (QOS) related services such as network lifetime, energy consumption, packet delivery ratio and throughput between Authenticated Anonymous Secure Routing (AASR), Reliable Minimum Energy Routing (RMER) and Multipath Routing Signature Protocol (MRSP). In MANET, node must be capable to interconnect each other to establish connection between source and destination. The results show that RMER performs well in terms of energy consumption, end to end delay and packet delivery ratio. After the analysis, this paper shows RMER performs well using 60 nodes in a network.

Index Terms: Routing, Routing protocols, Wireless sensor networks, Mobile ad hoc networks, Performance Analysis.

1. INTRODUCTION

Wireless sensor Network (WSN) has benefitted attention in both research and industry since they bring interaction between human, environment and machine. Most researchers define WSN is a network, which consists of autonomous nodes, cooperated nodes that sense, process and exchange data among the nodes. WSN rely on large number of devices that collaborate in distributed network combining data and processing the task. All the sensor nodes collaborate in a centralized processor and then send message to common sink.

It is impossible to deliver essential information with wired sensor networks in real time. However, the scenario differs with WSN where collection of data and real time processing can be done from remote environment. In addition, WSN play a vital role to deliver data from outside environment to centralized processor. Due to these characteristics, WSN can be deployed for dissimilar purposes in various environment. In WSN, the most basic components are the base stations and sensor nodes. These devices are battery operated and low cost. Due to simple design, they are closely restricted for storage, data processing and energy. Depending on the networks, sensor nodes pass the information to destination directly. The sensors measure the environmental conditions and process it to estimate the situation in the sensor surrounded area. Over long geographic area, large number of sensor nodes are deployed for precise monitoring. Although radio sensor node range is limited, it's a necessity to boost the size of network to cover larger area. Thus communication is possible via intermediate nodes.

Even though many routing protocols like DSR, AODV, TORA, DSDR and OLSR have been particularly designed for MANET which performed satisfactorily, WSN is a realization of MANET. However, MANET routing protocols implementation in Wireless Sensor Network is considered towards wireless ad hoc networks application. Although, finite research has been conducted on this yet it proves one of the best achievement of Mobile Ad hoc Network routing protocols on WSN.

Many researches attempted to solve multi-hop routing issue in WSN with multiple nodes and mobility. This paper provides performance analysis and comparison of hybrid routing protocols in various environment.

2. ROUTING PROTOCOLS

The three different routing protocols used in research to evaluate the performance and security analysis are listed below.

A. Authenticated Anonymous Secure Routing (AASR)

AASR uses group signature for authentication of RREQ per hop that prevents intermediate node from any modifications in the routing packet. Also AASR uses some common methods that are widely used. They are Trapdoor, Onion routing and Group signature.

Trapdoor defines an information collective mechanism where intermediate nodes add information like node IDs. However only destination and source can break & recover information using pre-generated secret keys. Also Trapdoor needs an unidentified end-to-end key between source and destination.

Onion routing provides private communication over public network. During data transfer, each node adds up with an encryption layer to route request (RREQ) message. There is no necessity that source and destination must know the ID of the forwarding nodes. The intermediate nodes validate its role by decryption process & by deleting onion's outer layer. Finally an unidentified route can be generated.

Group signature provides authentication. Every node in a group have a pair of private and public key issues by group head. The node may generate its own private key by their signatures and the same can be validated by other nodes of group without exposing the signer node's identity. Only authorized node in group can trace the signer node's identity and get back the group keys.

B. Reliable Minimum Energy Cost Routing (RMECR)

RMER routing protocol typically employ for data transmission in MANET networks. MANET nodes are free to move in any direction and hence there is a need of a routing protocol to maintain trustability and energy consumption. Furthermore the secure communications must be handed off securely without delays and drops. The routing protocol in the network is either end to end transmission or hop by hop transmission. In data transmission, data deploy from one node to the other depending on the energy level of each node in the route and the node with maximum energy level and trust level is selected for data routing. In case if a node encounters a hacker node then the RMECR routing employ sniffers to detect and delete hacker nodes in the network.

C. Multipath Routing Signature Protocol (MRSP)

MRSP signature routing protocol employ for secure data transmission to other nodes in a network. All the data transmitted from nodes are imprinted with a private and public keys. The receiver node receives and reads the message by decrypting the message with the attached public key. The node verifies the intended receiver by verifying the digital signature. If the signature matches the data is processed else the data is discarded. Furthermore,

the nodes are aware of secure data paths in the network making it easy for the next data to be transmitted with minimal end to end delay.

3. RESULTS AND DISCUSSION

The network performance of routing protocol evaluate with parameters namely throughput, end to end delay, energy consumption and packet delivery ratio.

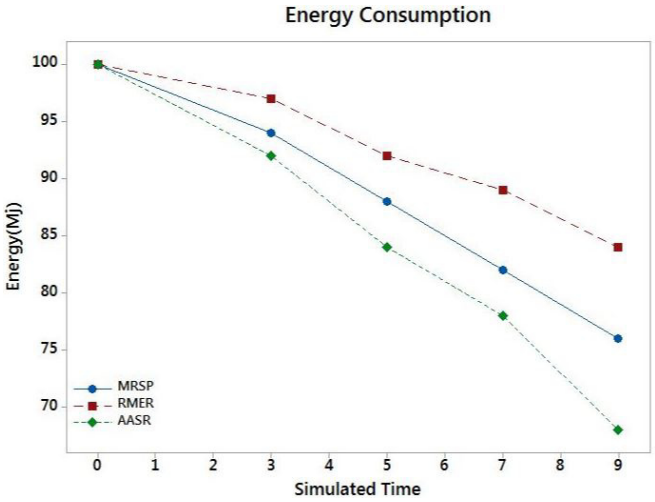

Figure 1: End to end delay

The end to end delay of AASR routing protocol is less compared to MRSP and RMER as shown in Figure 1. Since the routing protocol maintains a data base of trusted node ids in the network. The approach make it easy for next data to be easily transmitted without having to wait for node authentications.

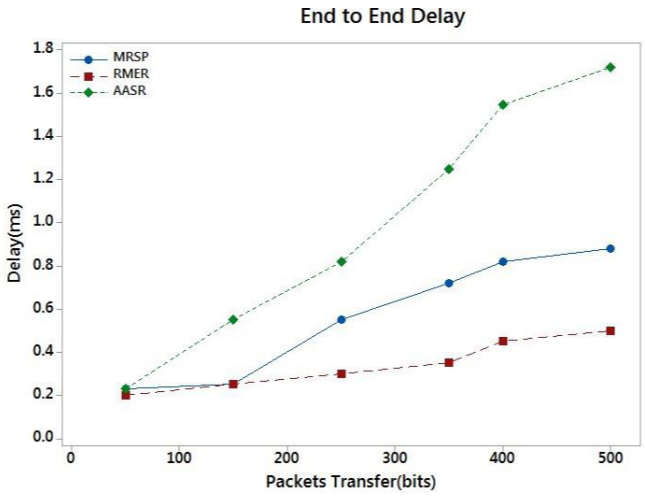

Figure 2: Energy consumption

The energy consumption of the network depends on the number of communications the node processes and the amount of data transferred through the node. The energy consumption is proportional to the data handled by the node as shown in Figure 2. The AASR routing protocol have a prolonged network life compared to other routing protocol. The earliest dead node occur at a instance 3 which is more compared to MRSP algorithm which occurs at 2.8 and RMER which occurs at 2.5.

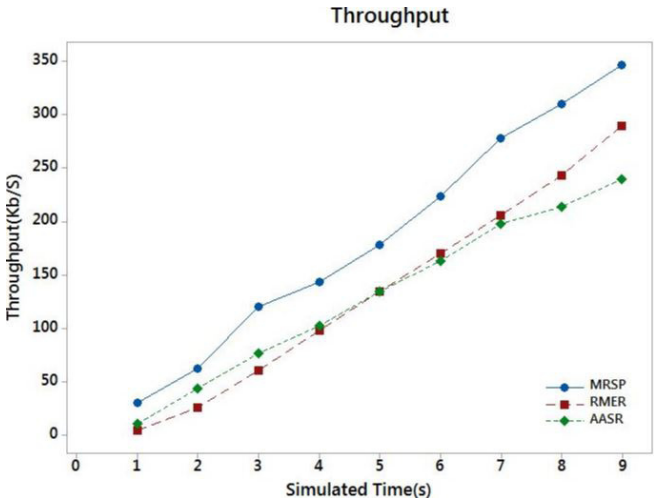

Figure 3: Throughput

The throughput of the network is the number of data's successfully received by the receiver from the transmitter. In the case, of throughput the MRSP algorithm has higher successful data transfer than compared to AASR and RMER routing protocols as shown in Figure 3. The throughput of MRSP is high since the routing protocol implements digital signature method for the data to successfully reach the desired receiver node.

Figure 4: Packet delivery ratio

The packet delivery ratio of RMER routing protocol is more since the routing protocol use trusted routes to transfer data to destination node compared to AASR and MRSP, which employ digital signature methods as shown in Figure 4. There is a deviation in output from packet delivery ratio and throughput since the nodes in the network are always free moving.

4. CONCLUSION

The paper summarises the performance of different routing protocols namely Authenticated Anonymous Secure Routing (AASR), Reliable Minimum Energy Cost Routing (RMECR) and Multipath Routing Signature Protocol (MRSP). The AASR routing protocol has 25% reduce end to end delay compared to MRSP and RMER routing protocol. In terms of energy consumption the AASR performs better than 39% compared to MRSP and RMER routing protocol. Furthermore, the MRSP routing protocol has higher throughput of 65% as opposed to RMER

with 59% and AASR routing protocol with 56%. However, RMER routing protocol performs well with 97% packet delivery ratio compared to MRSP with 75% and AASR with 60%.

REFERENCES

[1] C. Wang, J. Shih, B. Pan, and T. Wu, "A Network Lifetime Enhancement Method for Sink Relocation and Its Analysis in," Vol. 14, No. 6, pp. 1932–1943, 2014.

[2] T. Kim, S. H. Kim, J. Yang, S. Yoo, and D. Kim, "Neighbor Table Based Shortcut Tree Routing in ZigBee Wireless Networks," Vol. 25, No. 3, pp. 706–716, 2014.

[3] D. C. Hoang, S. Member, P. Yadav, and S. Member, "Real-Time Implementation of a Harmony Search Algorithm-Based Clustering Protocol for Energy-Efficient Wireless Sensor Networks," Vol. 10, No. 1, pp. 774–783, 2014.

[4] D. Djenouri and I. Balasingham, "Traffic-Differentiation-Based Modular QoS Localized Routing for Wireless Sensor Networks," Vol. 10, No. 6, pp. 797–809, 2011.

[5] J. Luo, J. Hu, D. Wu, R. Li, and S. Member, "Opportunistic Routing Algorithm for Relay Node Selection in Wireless Sensor Networks," Vol. 11, No. 1, pp. 112–121, 2015.

[6] A. E. Zonouz, S. Member, L. Xing, and S. Member, "Reliability-Oriented Single-Path Routing Protocols in Wireless Sensor Networks," No. C, 2014.

[7] F. Ren and T. He, "Traffic-Aware Dynamic Routing to Alleviate Congestion in Wireless Sensor Networks," Vol. 22, No. 9, pp. 1585–1599, 2011.

[8] J. Kim, J. Lee, H. K. Kang, D. S. Lim, C. S. Hong, S. Member, and S. Lee, "An ID / Locator Separation-Based Mobility Management Architecture for WSNs," Vol. 13, No. 10, pp. 2240–2254, 2014.

[9] G. Zhan, W. Shi, S. Member, and J. Deng, "Design and Implementation of TARF : A Trust-Aware Routing Framework for WSNs," Vol. 9, No. 2, pp. 184–197, 2012.

[10] D. Zhang, G. Li, K. Zheng, and X. Ming, "An Energy-Balanced Routing Method Based on Forward-Aware Factor for Wireless Sensor Networks," Vol. 10, No. 1, pp. 766–773, 2014.

[11] P. Bellavista, S. Member, G. Cardone, A. Corradi, and L. Foschini, "Convergence of MANET and WSN in IoT Urban Scenarios," Vol. 13, No. 10, pp. 3558–3567, 2013.

[12] W. Gu, N. Dutta, S. Chellappan, and X. Bai, "Providing End-to-End Secure Communications in Wireless Sensor Networks," Vol. 8, No. 3, pp. 205–218, 2011.

[13] H. Lin, L. Wang, and R. Kong, "Energy Efficient Clustering Protocol for Large - Scale Sensor Networks," No. 61501160, 2015.