ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

QART-MANET: Qualitative Analysis for Reliable Transmission of data using RAT Mechanism in MANET with 3DES Algorithm

[1] P.Emimal Gnana Merciba,[2] Dr. S.Balaji
[1] PG Student, [2] Professor&Head
[1][2] Department of Computer Science Engineering, Francis Xavier Engineering College, Vannarpettai, Tirunelveli

***Abstract* – In Mobile Ad-hoc Networks (MANET), a new framework is essential to reduce the network congestion that occurs when a network node is carrying data more than it can handle. The crucial problem includes in network congestion are packet loss, delay rate and insecurity of data. We propose a new framework called (QART) the Qualitative Analysis for Reliable Transmission of data using (RAT) the Rate Analysis for Traffic reduction Mechanism to overcome the impact of congestion using End-to-End explicit loss recovery. The base station makes the congestion detection, the rate adaptation and the rate allotment decisions to achieve greater efficiency. The RAT has the greater flexibility since many different traffic approaches can be implemented. In order to reduce the network communication overhead and improve message delivery success rate we presented (MHT) a Merkle Hash Tree algorithm based on the node distance to be measure. For the security of data 3DES technique for secure data transmission while maintaining the authenticity and integrity of the message. In this, message is encrypted before the data transmission process starts. The encryption and decryption of data is done by using the Triple Data Encryption Standard algorithm. Finally, performance of our proposed method has also been analyzed and compared with existing method for evaluation.**

Index Terms— Merkle Hash tree [MHT], Denial of Service [DOS], Triple Data Encryption Standard [3DES], Packet Loss, Delay Rate, Bandwidth.

I. INTRODUCTION

In Mobile Ad-hoc network, the wireless network which is used to exchange information. Each node is willing to forward data to other nodes. The network does not rely on fixed infrastructure and it is continuously self-configuring. MANETs consist of a peer-to-peer, self-forming, self-healing network. When a network node is carrying more than it can handle is the causes for the network congestion. It includes the packet loss, transmission delay and insecurity of data.

The packet loss occurs when one or more packets of data travelling across computer networks fail to reach their destination. The network delay rate specifies how long it takes for a bit of data to travel across the network from one node to another. Delay may differ slightly, depending on the location of the specific pair of communicating nodes.

Authentication is simply a process carried out by two parties in order to identify one another. Without authentication, an unauthorized node could easily "come in" and use the available resources within the network. The problem gets worse if the unauthorized node is a malicious user. Therefore, it is necessary to have a mechanism for preventing an "outsider" from being part of the network.

In this paper we discuss the design and implementation to develop a new adaptive rate congestion control mechanism that can prevent congestion and its subsequent issues in WSN and also to ensure low packet loss rate and end-to-end delay during data transmission from nodes to base station in order to maintain high QoS for real-time applications.

II. RELATED WORKS

In wireless ad-hoc [1] networks, the communications between D2D have congestion. The D2D approach does not offers very significant throughput gains with respect to base station. [2]The D2D communication is conceived as a vital component for next-generation wireless networks by requiring nodes to stay asleep when the possibility that it successfully contacts another node is relatively high. [3] But the D2D communication systems, which does not assume the system to be in saturated conditions. The coupled proc
essors model to describe a cellular scenario with D2D users for the determination of fair resource allocation. [4] The concept for securing data transmission before allocation is required. But the OTPs are complicated to

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

handle for each bit of plain text data, another bit of OTP must be available. [5-6] The network performance improvement causes path-loss after the resource allocation in D2D and also the distance variations caused by node mobility generate fluctuations in the channel gains. They can be treated as a type of fading besides multipath effects. [7]During fading and the multi-path the routing protocols such as DSDV helps security level in the network and thus avoid any malicious nodes or untrusted nodes. It also reduces the power consumption by using the trust factor. But the occurrence of fading is not reduced. [8] The SINR (signal to interference plus noise ratio) is a key factor for wireless networks analysis. By using propagation model which takes into account only the path loss where SINR is directly derived from the CDF (cumulative distributed function). [9-12] The problem of how social selfishness influences the performance of epidemic routing in DTN. The message delivery process including with social selfishness as a two dimensional continuous time Markov chain. The DTN is quite robust to social selfishness. The routing method then becomes a hypercube–based feature matching process to protect routing efficiency. Since routing in DTNs is thus challenging since it must handle network partitioning, long delays, and dynamic topology in such networks.[13]ID-based encryption for secure data transmission is a routing protocol that maintains the best hop information in its routing table.[14] The reliability of a wireless sensor network executing a distributed code attestation protocol with neighbor sensor nodes serving as code verifiers.[15] Device-to-device (D2D) communication underlying cellular networks algorithms especially in terms of achievable throughput even with markedly reduced complexity levels.

III. METHODOLOGY

A. Contributions

In our paper we develop a framework of resolving the network congestion. It may cause packet loss, resulting in queuing delay and blocking of new connection. We consider the packets sending by the nodes are inserted in the queue. Here queue is the collection of data packets waiting to be transmitted by a network device based on the priority of the data packets in the queue. We proposed a new mechanism which has the primary goal to achieve the end-to-end reliability. The RAT mechanism is used for the congestion detection. It uses threshold technique for time to recover loss by round trip time. In response to congestion it adapts to transmission rates. So RAT mechanism's rate adaptation design uses the total sustainable traffic, increase and decrease formula for making rate adaptation decisions. The mechanism then estimates the loss rate using average loss interval to control congestion. Therefore the rate allocation components of RAT mechanism to implement the capacity allocation approach. This components consist of three different approaches Demand proportional, Demand limited and Fair to define the capacity allocation approach of the Rate allocation component. The data authentication can be performed by the Encryption and decryption algorithm. These all were explained in the following sections.

B. End-to-End Reliability

RAT implements a NACK-based end-to-end loss recovery scheme to guarantee 100% reliable data delivery, Unlike TCP. From the mobile source node, the BS detects packet losses and repairs them by requesting end-to-end retransmissions. Here, BS has the more memory and it keep track of all the missing packets. The mobile node of each stores a copy of the data packets in its local retransmit buffer when the process of the packet transmission to the BS. Hence the BS keeps track of the packets sequence numbers that it receives on each flow.

The packet loss can be indicated by the arise of gap in the sequence number of received packets. The BS also maintains the missing packets list per each flow. The sequence numbers of the lost packets are inserted into the list when the losses are detected. By the BS to each source the entries in this list of missing packets are sent as the Negative-Acknowledgements (NACKs). The ACK implosions are avoided by using the NACKs, when the BS overwhelms the network sent the acknowledgments of successful receptions.

Fig 1 shows that the source retransmits the requested packets to repair the losses while receiving a NACK. Also, by looking at the cumulative ACK sequence numbers piggybacked in all feedback packets have the source determines when it can safely overwrite packets in the retransmit buffer.

To provide in-order delivery of data packets to the application the BS also maintains a list of out-of-order packets for each flow. This list contains packets that are received at the BS but have not been passed to the application layer because there are one or more gaps in the sequence numbers.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

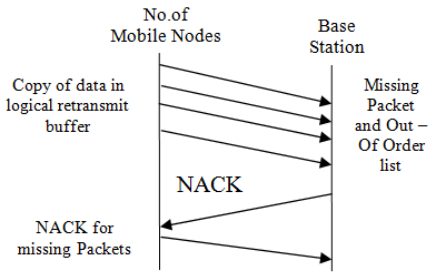


Fig 1 End-to-End Reliability

For example, if sequence numbers [0, 1, 2, 3, 5, and 6] have been received so far, packets 4 and 5 are inserted into the out-of-order packets list. When packet 4 is received, the BS passes packets 3, 4, 5 to the application and removes 4, 5 from the out-of-order packets list. As we shall discuss below, The RAT uses the per-flow lists of missing and out-of-order packets for detecting congestion and adapting rates. Figure 2 shows the overall architecture of the QART-MANET mechanism.

QART-MANET Algorithm
Algorithm QART- MANET
  If Congestion Detection in Ns == TRUE
    Call Congestion Control
  Else
    If Delay == TRUE
      Call Delay-tolerant node selfishness
    Else
      If Authenticated OTP-Pads== TRUE
        Call Decryption
        Deliver data
      Else
        Drop data
      End
    End
  End
End

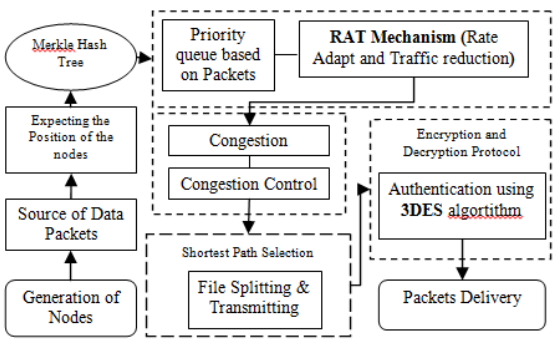


Fig 2 QART-MANET Architecture

IV. PROTOCOL OVERVIEW

Our QART incorporates the way toward creating a mark by a sender and confirming the mark by a collector. We present them independently.

To begin with, every hub parts its course of events into a grouping of time spans. Each time allotment is additionally separated into a grouping of signal interims, which we comment I 0, I1, •••, In. In a time period, to send the principal reference point B 0 for I0, a vehicle will perform four stages: fastened keys age, position desire, Merkle Hash Tree Development, and mark age

1. Chained Keys Generation

Toward the start of a time allotment, every gadget creates n affixed private keys for the following n reference points. It utilizes one interim worth of private key for verification as the 3DES plan. 3DES plan to help moment confirmation, which enables the beneficiary to check bundles when they arrive.

2. Position Expectation

At each reference point interim, every gadget expects its position communicate in the following signal. To do as such, gadget display all the conceivable aftereffects of developments between two back to back reference points in light of data of the past direction

3. Merkle Hash Tree Development

After position desire, the hub will develop one interim worth of an open key and private keys. These private keys are related with the consequences of developments. We propose a MHT, which ties these pre-processed keys together and afterward produces a solitary open key or desire result for all the conceivable developments.

4. Signature Generation

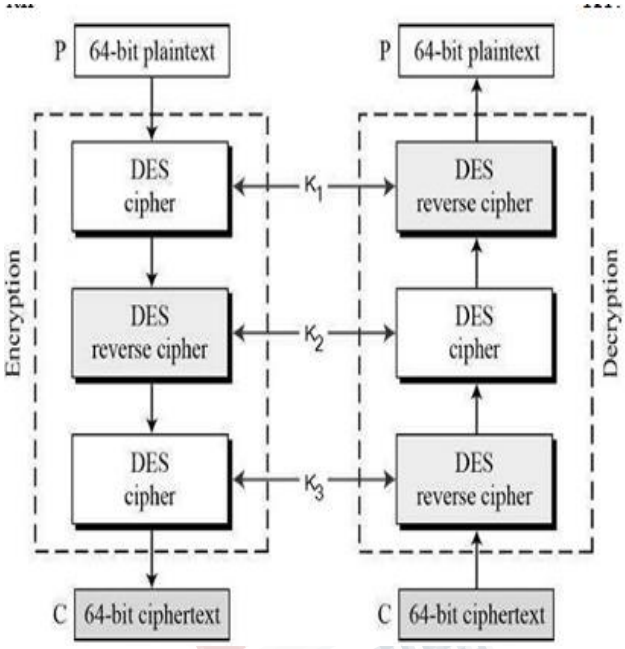
After position desire and MHT development, the hub signs the dedication of the hash chain and the desire result from MHT utilizing DES marks, and communicates it alongside the principal reference point B0 in the time period. For whatever is left of guides, for example, B1, B2, •••, Bn, the hub signs the message and the desire result from MHT utilizing the DES keys relegated in the interims I1, I2, •••, In. The 3DES (Triple DES) encryption standard was proposed in this standard the encryption strategy is like the one in unique DES yet connected 3 times to expand the encryption level.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

The encryption-unscrambling process is as per the following −

• Encrypt the plaintext squares utilizing single DES with key K1.
• Now decode the yield of stage 1 utilizing single DES with key K2.
• Finally, encode the yield of stage 2 utilizing single DES with key K3.
• The yield of stage 3 is the figure content.
• Decryption of a figure content is a switch procedure. Client initially decode
• Using K3, at that point encode with K2, lastly decode with K1.



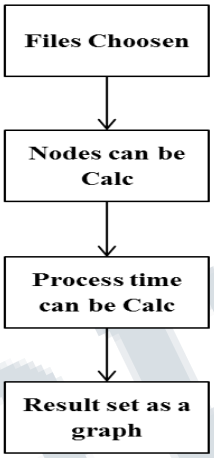
(C) 3DES Standard

Because of this plan of Triple DES as an encrypt–decrypt– scramble process, it is conceivable to utilize a 3TDES (equipment) usage for single DES by setting K1, K2, and K3 to be a similar esteem. This furnishes in reverse similarity with DES.

3DES frameworks are essentially more secure than 1DES, yet these are unmistakably a much slower process than encryption utilizing 1DES.

5. Bandwidth Allocation

In Data transmission assignment technique the transfer speed can be ascertained between various hubs and the procedure time can be figured. At that point the outcome can be figured to make as a diagram.



(D) Bandwidth Workflow

V. RESULTS AND DISCUSSION

From the analysis of performance evaluation graph comparing with other methods QART method gives the better result. When its cryptographic, communication level and DoS attack protection is higher than other methods. And also packet loss and delay is low so it gives good data communication with best protection .The below table explains the overall value and the requirement parameters for this method.

VI. CONCLUSION

In this paper, a comparative performance review of different MANET routing protocols QART including proactive (DSDV), and reactive (AODV) protocols is done. The simulated experiments were performed with increasing speed of mobile nodes from 10m/s to 40m/s. We propose an effective, efficient and scalable broadcast authentication scheme to provide both computation-based DoS attacks resilient and packet losses resilient in MANETs. To defend against memory based DoS attacks. QART has been demonstrated to perform well even under high-density traffic scenarios and lossy wireless scenarios. In the future work we will satisfy privacy requirements and improve accurate measurement models.

ACKNOWLEDGMENT

This paper was supported by the Francis Xavier College of Engineering, Final Year PG Computer Science and

Engineering student P.Emimal Gnana Merciba (Reg.no: 950716405003) guided by Professor & Head of Computer Science and Engineering Dr. S.Balaji. The authors thank to their colleagues for their help and support at different stages of the system development. Finally, we would like to thank the anonymous reviewers for their helpful comments.

REFERENCES

[1]G. Holland, N. Vaidya, and P. Bahl, "A rate-adaptive MAC protocol for multi-hop wireless networks," in Proc. ACM MobiCom, 2001, pp. 236–251.

[2]C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," IEEE Trans. Mobile Comput., vol. 2, no. 3, pp. 257–269, Jul.–Sep. 2003.

[3]A.Zanella, M. Stramazzotti, F. Fabbri, E. Salbaroli, D. Dardari, and R. Verdone, "Comments on "probability distributions for the number of radio transceivers which can communicate with one another"," IEEE Transactions on Communications, vol. 46, no. 5, pp. 1287–1289, May 2009.

[4] Y. Li, P. Hui, D. Jin, L. Su, L. Zeng, "Evaluating the impact of social selfishness on the epidemic routing in delay tolerant networks". IEEE Communications Letters 14(11), 1026–1028 ,2010.

[5] L. Hanzo and R. Tafazolli, "QoS-aware routing and admission control in shadow-fading environments for multirate MANETs," IEEE Trans. Mobile Comput., vol. 10, no. 5, pp. 622–637, May 2011.

[6]I.R. Chen and Y. Wang, "Reliability Analysis of Wireless Sensor Networks with Distributed Code Attestation," IEEE Communications Letters, vol. 16, no. 10, 2012, pp. 1640-1643.

[7]D. Feng, L. Lu, Y. Yuan-Wu, G. Li, G. Feng, and S. Li, "Device-to-device communications underlaying cellular networks," IEEE Transactions on Communications, vol. 61, no. 8, pp. 3541–3551, August 2013.

[8]M. Almasri, K. Elleithy, A. Bushang, and R. Alshinina, "TERP: A Trusted and Energy Efficient Routing Protocol for Wireless Sensor Networks (WSNs)." IEEE, Oct. 2013, pp. 207–214.

[9]S. Balaji, M. Rajaram, Y. Harold Robinson, E. Golden Julie, "A Hypercube Social Feature Extraction and Multipath Routing in Delay Tolerant Networks", in International Science Index, Computer and Information Engineering Vol:10, No:6, 2016.