International Journal of Mechanical Engineering Research (IJMER)
Volume 1, Issue 3, September 2020, Pages 30-35

Balancing the Energy Consumption and Data Integrity in MANET

G. Sathya
Assistant Professor
SNS College of Engineering
sathya_g82@yahoo.co.in

P. Kalaivani,
Assistant Professor,
SNS College of Engineering
Engineeringpkalai.ece@gmail.com

N. Senthilnathan
Chief Architech
Robert Bosch,Coimbatore.
Senthilnathan.nagarajan@in.bosch.com

ABSTRACT

Nowadays most of the existing data replication solutions in both wired and wireless networks aim at either by reducing the query delay or improving the data availability. These parameters are monitored continuously with the help of corresponding data replications techniques. To balance the trade off between the query delay and data availability in MANET, it is evaluated under different system settings and requirements. If the cooperation of the nodes are not connected properly, it will lead to link failures and node failures. So the motivation of Data Replication technique is to analyse the delay, probabability of the link failures and data availability with the help of data replication schemes like greedy data replication, one to one optimization scheme and reliable neighbor scheme. Here the degree of connectivity, cooperation among the nodes, node failures are analysed.

1. INTRODUCTION

1.1 DATA AVAILABILITY AND NEED OF DATA REPLICATION

Data availability means where the availability ensures that the data can be successfully transmitted from the source to the destination in a timely manner. It is assumed that the application layer does not use encryption and expects the underlying network services to be secure. Data Replication is technique which enhances data availability by making copies of data items. Furthermore there are various issues arise in MANET which leads to problem in data replication. Replication allows better data sharing. It is a key approach for achieving high availability[4]. It is suitable to improve the response time of the access requests, to distribute the load of processing of these requests on several servers and to avoid the overload of the routes of communication to a unique server[2].

1.2 THE MAIN CAUSES ON DATA AVAILABILITY

Existing Wireless Local Area Network (WLAN) standards, such as IEEE 802.11 , do not employ physical layer error correction, which makes them trivial targets for Denial-of-Service (DoS) attacks. For example, an attacker only needs to jam one bit to induce failure of the Cyclic Redundancy Check (CRC). Hence, the jammer needs to expend several orders of magnitude less energy than a legitimate sender. It is likely that a small number of coordinated jammers can launch very harmful attacks with only limited energy resources. For instance, this group of jammers may be able to prevent all network communications, partition the network, or force traffic to be routed over a particular network region, where an adversary has powerful equipment for encryption cracking or traffic analysis [3].

The use of multipath routing with data redundancy can statistically enhance data availability. If one or more paths are jammed, it may still be possible to reconstruct an end-to-end message from the information carried by the remaining paths. However the physical proximity of the chosen paths must be taken into account such that multiple node-disjoint paths are spatially far apart. This can be accomplished by choosing paths with low correlation [4]. All network traffic going through nodes within these regions were dropped. It was found that the use of less-correlated paths significantly increases the probability that at least one end-to-end route remains operational, especially as the radius R increases. Therefore, it is likely that minimizing the path-set correlation factor will improve resilience to jamming by decreasing the probability that all or most of the path between the source and destination can be jammed. It should be noted that physical jamming is an aggressive form of active attack that can be readily detected by electronic means. Hence, the adversary can be quickly forced to cease the attack, since the source of the jamming signals can be precisely determined. On the other hand, eavesdropping cannot be detected unless the adversary is physically located. Consequently, the adversary may covertly snoop network traffic for lengthy periods of time[2]. It is much more difficult to maintain data confidentiality than data availability with respect to outsider's attack[3].

1.3 ISSUES CONCERNING DATA ACCESSIBILITY

Data accessibility means that the number of successfully serviced requests divided by the total number of data item requests generated by all mobile hosts in the network. Some of the following major issues concerning data accessibility is given below:

• *Frequent disconnection of mobile hosts*: Mobile hosts often get disconnected from the network due to various factors like power failure or their mobility. Some mobile users switch their units on and off regularly to save power, causing more network disconnections. Servers which hold the data cannot provide services if they are disconnected from other mobile hosts. Thus, ideally, the replication algorithm should determine when a particular mobile host would be disconnected and, accordingly, replicate its data items in a different server to improve data accessibility [17 -19].

• *Network partitioning*: Due to frequent disconnection of mobile hosts, network partitioning occurs more often in MANET databases than in traditional databases. Network partitioning is a severe problem in MANET when the server that contains the required data is isolated in a separate partition, thus reducing data accessibility to a large extent. Therefore, the replication technique should be able to determine the time at which network partitioning might occur and replicate data items beforehand.[1][2]

1.4 REPLICATED DIGITAL SIGNATURE TECHNIQUE

The proposed technique consists of the following modules

i. Integrated Encryption and Decryption Scheme
ii. Energy Consumption Model.

1.4.1 Integrated Encryption and Decryption Scheme

In IEDS, a Diffie-Hellman shared secret is used to derive two symmetric keys k_1 and k_2. Key $k1$ is used to encrypt the plaintext using a symmetric-key cipher, while key k_2 is used to authenticate the resulting cipher text. Intuitively, the authentication guards against chosen-cipher text attacks since the adversary cannot generate valid ciphertexts on her own. The following cryptographic primitives are used:

1. KDF is a key derivation function that is constructed from a hash function H. If a key of l bits is required then KDF(S) is defined to be the concatenation of the hash values $H(S, i)$, where i is a counter that is incremented for each hash function evaluation until l bits of hash values have been generated.

2. ENC is the encryption function for a symmetric-key encryption scheme such as the Advanced Encryption Standard (AES).

3. MAC is a message authentication code algorithm such as HMAC.

Encryption and Decryption works If ciphertext (R,C, t) was indeed generated by the legitimate entity when encrypting m, then $hdR = hd(kP) = hk(dP) = hkQ$. Thus the decryptor computes the same keys $(k1, k2)$ as the encryptor, accepts the ciphertext, and recovers m.

The shared secret point $Z = hdR$ is obtained by multiplying the Diffie-Hellman shared secret dkP by h. This ensures that Z is a point in the subgroup. Checking that Z =∞ in step 2 of the decryption procedure confirms that Z has order exactly n. This, together with embedded key validation performed which provides resistance to the small subgroup and invalid-curve attacks described whereby an attacker learns information about the receiver's private key by sending invalid points R[8, 20, 21].

The symmetric keys k_1 and k_2 are derived from the x-coordinate x_Z of the Diffie-Hellman shared secret Z as well as the one-time public key R of the sender. Inclusion of R as input to KDF is necessary because otherwise the scheme is malleable and hence also not indistinguishable[11]. An adversary could simply replace R in the cipher text (R, C, t) by $-R$ thus obtaining another valid cipher text with the same plaintext as the original cipher text[4, 22-25].

1.4.2 Minimum Energy consumption Model

In order to consider the energy const for the path of minimum energy consumption, we developed minimum energy consumption model. Here each mobile host dynamically changes the weight which is based on the path lengths to its nearby hosts. The following is the behavior of the method when*Mi* accesses *Dnew*, which is not held by itself.

1. Here, the data information reply packet includes the information on the path length from *Mi* to *Mk*.
2. If*Mi* receives reply packets, it calculates the following criterion, $\Delta i,j \rightarrow new$, for each data item held by *Mi*:

$$\Delta_{p,q\rightarrow new}$$

$$= \beta(a_{p,new} - a_{p,q}) + \alpha \frac{\sum r \in T_{fresh}}{E_i} + .\lambda\left(\frac{A'_{k,fresh}}{U_{k,fresh}+1} - \frac{A'_{k,l}}{U_{k,l}}\right)$$

The Received and Transmitted energy of the proposed model is

$$Ptop\_Tx(vj\text{-}1) =$$

$$Transenergy\left(\frac{Sizeof\mathrm{Re}qToSend + Sizeoforiginaldata + PDR}{Bandwidth}\right)$$

$$+$$

$$\mathrm{Rec}eenergy*\left(\frac{SizeofCleartosend + Acksize + RERR}{Bandwidth}\right)$$

$$Ptop\_Rec(vj\text{-}1) =$$

$$Transenergy\left(\frac{SizeofClearToSend + ACKsize + RERR}{Bandwidth}\right)$$

$$+$$

$$\mathrm{Re}ceenergy * \left(\frac{Sizeof\ \mathrm{Re}qtosend + Datasize + PDR}{Bandwidth}\right)$$

Here, *Gj* denotes the set of mobile hosts within *h* hops that do not hold *Dj* and *hk* denotes the path length from *Mi* to *Mk*.

3. *Mi* selects *Dj* among its own data items so that *Δi,j→new* has the positive maximum value and replaces *Dj* with *Dnew*.

The minimum energy consumption model prevents mobile hosts from being accessed by far away hosts. This method can adjust data availability and power consumption by changing parameters *α*, and *β*.

The proposed algorithm determines the energy conservation rate based on the above three factors and also the total number of bits transmitted per energy.

$$E_{CR} = \sum(T_{mb}, T_{tv}, DS_{\min}) + \frac{\chi_{BR}}{\sum \delta_{es}(t)}$$

χ_{BR} - Number of bits transmitted (bits).

$\sum \delta_{es}(t)$ - Total energy consumed (Joules).

T_{mb} – Trust Mobility factor

T_{tv} – Trust threshold vector value

DS_{min} - Minimum Digital Signature

From the analysis of the proposed scheme, the energy efficiency of the node is well improved and the data integrity of the networks is getting more. The proposed scheme makes balance between the energy consumption, data availability and data integrity.

2. RESULTS AND DISCUSSION

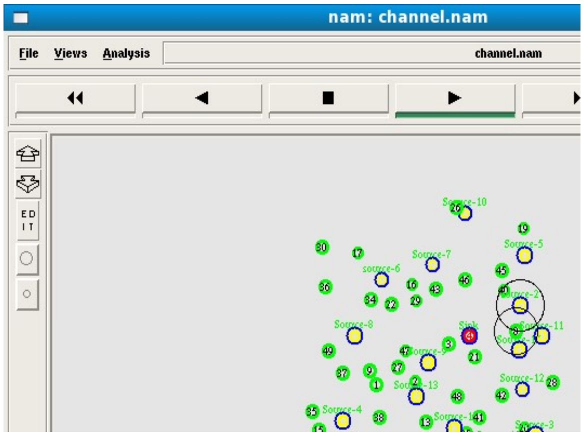
2.1 Simulation Result

2.1.1 Scenario characteristics

Channel Type	Channel/Wireless Channel
Radio-Propagation Model	Propagation / Two Ray Ground
Antenna Type	Antenna / Omni Directional Antenna
Interface Queue Type	Priqueue
Max Packet In Ifq	250
Network Interface Type	Phy/Wirelessphy
Mac	Mac/802_11
Number of Mobile Nodes	50
Routing Protocol	AOMDV
Simulation End Time	50 (Sec)
Node Speed	30(Meters/Sec)
Radio Range	250 meters
Pause time	50 sec

Table.2.1: Simulation Parameters

Node setup



2.2.When Tuning the Mobility:

2.2.1 Mobolity Vs packet authentication ratio

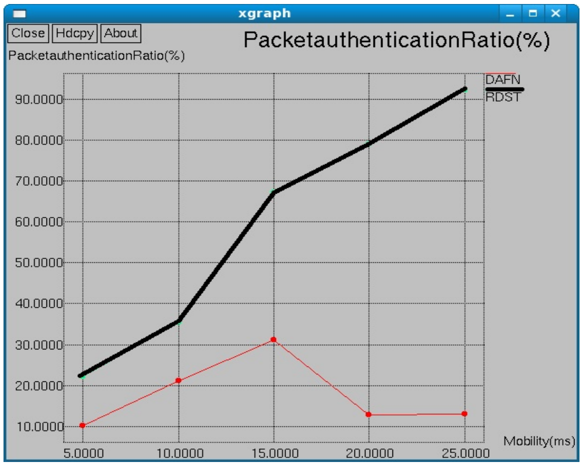


Fig.2.2. Mobility Vs Packet Authentication Ratio

Table 2.2: Comparison of protocols(Mobility Vs Packet Authentication Ratio)

2.3 When Increasing the no of Nodes:

2.3.1 No of nodes Vs connectivity ratio

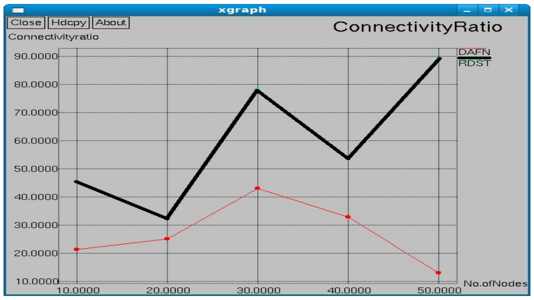


Fig.3.3. No. of Nodes Vs Connectivity Ratio

NO OF NODES	CONNECTIVITY RATIO	
	DAFN	RDST
10	21	46
20	26	32
30	43	78
40	32	53
50	12	89

Table 3.3: Comparison of protocols(No. of Nodes Vs Connectivity Ratio)

2.4 When Increasing the Time:

2.4.1 Time Vs Data availability ratio

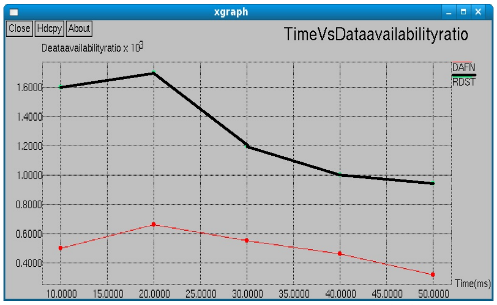
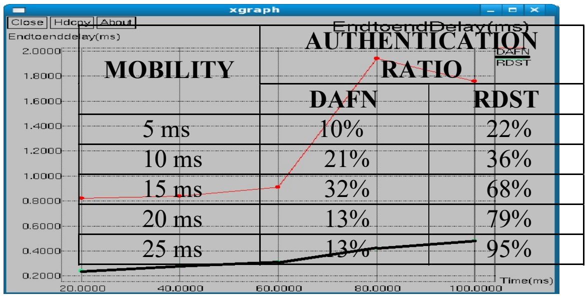


Fig.2.4.1. Time Vs Data Availability Ratio

TIME(ms)	DATA AVAILABILITY RATIO	
	DAFN	RDST
10	0.512	1.602
15	0.588	1.645
20	0.686	1.709
25	0.624	1.428
30	0.583	1.199
35	0.528	1.000
40	0.487	0.899
45	0.389	0.889
50	0.314	0.880

Table 2.4: Comparison of protocols(Time Vs Data Availability Ratio)

2.4.2 Time Vs end to end delay



MOBILITY	AUTHENTICATION RATIO	
	DAFN	RDST
5 ms	10%	22%
10 ms	21%	36%
15 ms	32%	68%
20 ms	13%	79%
25 ms	13%	95%

Fig 2.4.2. Time Vs End to end delay

TIME(ms)	END TO END DELAY (ms)	
	DAFN	RDST
20	0.812	0.221
40	0.822	0.289
60	0.915	0.323
80	1.886	0.411
100	1.786	0.495

Table 2.4.2: Comparison of protocols(Time Vs End to end Delay)

2.4.3 Time Vs throughput

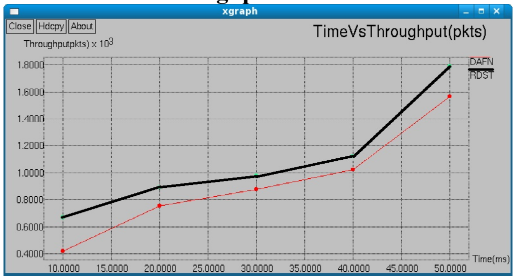


Fig.2.4.3. Time Vs Throughput

TIME	THROUGHPUT	
	DAFN	RDST
10	0.411	0.632
15	0.589	0.788
20	0.785	0.899
25	0.821	0.912
30	0.845	0.984
35	0.976	1.221
40	1.119	1.654
45	0.295	1.425
50	1.589	1.798

Table 2.4.3: Comparison of protocols(Time Vs Throughput)

2.5 When Increasing the Speed:

2.5.1 Speed Vs Delivery Ratio

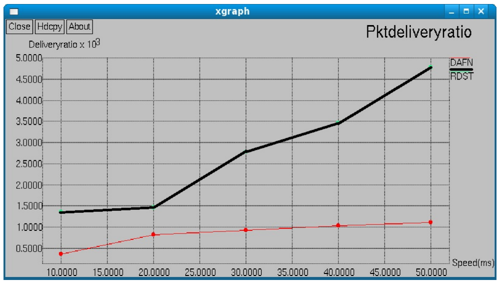


Fig2.5.1. Speed Vs Packet Delivery Ratio

SPEED	DELIVERY RATIO	
	DAFN	RDST
10	0.485	1.472
15	0.515	1.486
20	0.755	1.498
25	0.828	2.198
30	0.958	2.669
35	0.999	3.213
40	1.002	3.498
45	1.123	4.196
50	1.211	4.565

Table 2.5.1: Comparison of protocols(Speed Vs Delivery Ratio)

:

3. CONCLUSION

The balance between the data integrity, data availability ratio and energy consumption using Replicated Digital Signature Technique (RDST) is improved in MANET. The simulation results show that proposed scheme in terms of end to end delay, overhead, throughput, network connectivity ratio, packet authentication ratio and data availability ratio for more security in MANET.

REFERENCES

[1] P. Kalaivani, G. Sathya, and N. Senthilnathan, “Dynamic Data Routing in manet using position based opportunistic Routing Protocol,” International Journal of research in computer Applications & Robotics (IJRCAR), vol. 2, Issue12, Dec- 2014.

[2] P.Kalaivani ,G.Sathya, N. Senthilnathan, “Qos Parameters Estimation in MANET Using Position Based Opportunistic Routing Protocol” on American Journal of Computer Science and Engineering Survey, ISSN 2349 – 7238.

[3] T. Hara, “Effective Replica Allocation in Ad Hoc Networks for Improving Data Accessibility,” Proc. IEEE INFOCOM, 2001.

[4] C.-Y. Chang, C.-T. Chang, and S.-C. Tu. Obstacle-free geocasting protocols for single/multi-destination short message services in ad hoc networks. Wirel. Netw., 9(2):143–155, 2003.

[5] Y.-B. Ko and N. H. Vaidya. Geocasting in mobile ad hoc networks: Location-based multicast algorithms. In WMCSA ’99: Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications, page 101, Washington, DC, USA, 1999.IEEE Computer Society.

[6] V. Ramany and P. Bertok, “Replication of location-dependent data in mobile ad hoc networks,” ACM MobiDE, pp. 39–46, 2008.

[7] Bellavista, P., Corradi, A., Magistretti, E.: REDMAN: A decentralized middleware solution for cooperative replication in dense MANETs. In: International Conference on Pervasive Computing and Communications Workshops, 2005, pp. 158–162.

[8] Bellavista, P., Corradi, A., Magistretti, E., “ Comparing and evaluating lightweight solutions for replica dissemination and retrieval in denseMANETs”, In: IEEE International Symposium on Computers and Communications, 2005, pp. 43–50.

[9] Luo, J., Hubaux, J.P., Eugster, P.T.: PAN: Providing reliable storage in mobile ad hoc networks with probabilistic quorum systems. MobiHoc, 2003, pp. 1–12.

[10] Tamori,M., Ishihara, S.,Watanabe, T., Mizuno, T.:A replica distribution method with consideration of the positions of mobile hosts on wireless ad hoc networks. In: International Conference on Distributed Computing Workshops, 2002, pp. 331–335.

[11] Yang Zhang, Liangzhong Yin, Jing Zhao and Guohong Cao, “Balancing the Trade-Offs between Query Delay and Data Availability in MANETs”, IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 4, April 2012, pp.643-650.

[12] B. Tang, H. Gupta, and S. Das, “Benefit-Based Data Caching in Ad Hoc Networks,” IEEE Trans. Mobile Computing, vol. 7, no. 3, pp. 289-304, Mar. 2008.

[13] Baev and R. Rajaraman, “Approximation Algorithms for Data Placement in Arbitrary Networks,” Proc. 12th Ann. ACM-SIAM Symp. Discrete Algorithms (ACM-SIAM SODA), pp. 661-670, 2001.

[14] T. Hara and S. Madria, “Consistency Management Strategies for Data Replication in Mobile Ad Hoc Networks,” IEEE Trans. Mobile Computing, vol. 8, no. 7, pp. 950-967, July 2009.

[15] J. Cao, Y. Zhang, G. Cao, and L. Xie, “Data Consistency for Cooperative Caching in Mobile Environments,” Computer, vol. 40, no. 4, pp. 60-66, Apr. 2007.

[16] T. Hara, “Effective Replica Allocation in Ad Hoc Networks for Improving Data Accessibility,” Proc. IEEE INFOCOM, 2001.

[17] Boselin Prabhu, SR & Sophia, S, 2012, ‘A research on decentralized clustering algorithms for dense wireless sensor networks’, International Journal of Computer Applications, vol. 57, no. 20, pp. 35-40.

[18] Boselin Prabhu, SR & Sophia, S, 2013, ‘Mobility assisted dynamic routing for mobile wireless sensor networks’, International Journal of Advanced Information Technology, vol. 3, no. 3, pp. 9-19.

[19] Boselin Prabhu, SR & Sophia, S, 2013, ‘A review of energy efficient clustering algorithm for connecting wireless sensor network fields’, International Journal of Engineering Research and Technology, vol. 2, no. 4, pp. 477-481.

[20] Boselin Prabhu, SR & Sophia, S, 2013, ‘Variable power energy efficient clustering for wireless sensor networks’, Australian Journal of Basic and Applied Sciences, vol. 7, no. 7, pp. 423-434.

[21] Boselin Prabhu, SR & Sophia, S, 2013, 'Capacity based clustering model for dense wireless sensor networks', International Journal of Computer Science and Business Informatics, vol. 5, no. 1, pp. 1-10.

[22] Boselin Prabhu, SR & Sophia, S, 2013, 'Hierarchical distributed clustering algorithm for energy efficient wireless sensor networks', International Journal of Research in Information Technology, vol. 1, no. 12, pp. 45-55.

[23] Boselin Prabhu, SR & Sophia, S, 2013, 'Real-world applications of distributed clustering mechanism in dense wireless sensor networks', International Journal of Computing Communications and Networking, vol. 2, no. 4, pp. 99-105.

[24] Boselin Prabhu, SR & Sophia, S, 2013, 'An integrated distributed clustering algorithm for dense WSNs', International Journal of Computer Science and Business Informatics, vol. 8, no. 1, pp. 1-12.

[25] Boselin Prabhu, SR & Sophia, S, 2014, 'Modern cluster integration of advanced weapon system and wireless sensor based combat system', Scholars Journal of Engineering and Technology, vol. 2, no. 6A, pp. 786-794.