ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(14), DOI: 10.17485/ijst/2016/v9i14/90204, April 2016* ISSN (Online) : 0974-5645

Integrity Key based Mechanism to Debase Packet Dropping in Manets

S. Sasila Jabamani* and E. Rajinikanth

Department of ETCE, Sathyabama University, Chennai - 600119, Tamil Nadu, India;
sasilajm@gmail.com, rajinikanth4@gmail.com

Abstract

Background: MANETS are intrinsically insecure, subsequently they are powerless and pernicious to aggressors and outer ruinous variables can results in loss of bundles to the destination hub. Methods: On the other hand, MANETS have restricted energy ideal utilization of vitality for improving network lifetime is of high importance. In this paper a convention in view of ID based encryption to debase packet dropping in MANETS. **Findings:** This calculation takes the parameters of packet delivery proportion, throughput and transmission delay into record. In this encryption technique, one of a kind ID is given to all nodes in the system utilizing ID based encryption strategy. So after each transmission key gets upgraded to the system. On the off chance that any of the node drops the packet in the sense, we can ready to distinguish it quickly. **Improvements:** This system minimizes the packet misfortune. Hence node energy utilization is diminished. The recreation results uncovered that using the ID based encryption procedure in the proposed strategy results in high packet delivery proportion. In this way the reenactment results demonstrate that the proposed technique prompts higher packet delivery proportion, throughput and lower transmission delay.

Keywords: ID based Encryption, MANETS, Packet Delivery Proportion, Throughput, Transmission Delay

1. Introduction

Mobile Ad hoc Network (MANET) is broadly utilized as a part of emergency administration administrations, for example, military operation and debacle salvage programs furthermore in satellite correspondence and Personal Area Networks. The utilization of MANET for business reasons for existing is at present being investigated. As of late MANET is likewise being utilized in Internet of Things (IOT) Body Area Network (BAN and 5G devices)[1–5]. Its self making, self sorting out and self controlling ability and foundation less element makes it favorable than contemporary system, for example, wired, remote and portable network[6,7]. Figure 1 represents the fundamental structure of Mobile Ad hoc Network. Lamentably, the open medium and remote dispersion of MANET make it helpless against different sorts of assaults. For instance because of the hubs, absence of physical properties, vindictive assailants can without much of a stretch catch and bargain hubs to accomplish attacks[8,9]. Specifically, Considering the way that most steering conventions in MANETS expect that each hub in the system carries on co-operatively with different hubs and apparently not malevolent, assailants can without much of a stretch trade off MANETS by embeddings misbebavior[10,12] or non co-agent hubs into the system. Besides, as a result of MANET's dispersed engineering and evolving topology, a customary concentrated checking method is no more achievable in MANETS. Since parcel misfortune data is exceptionally touchy and can be focused by the assailants keeping in mind the end goal to hurt the system or the application running in the system.

2. Related Work

A few works have been done for enhancing the packet delivery ratio, throughput and to lessen the delay. On the off chance that MANET can recognize the aggressors when they enter the system, we will ready to totally wipe out the potential harms created by bargained nodes at the first run through. Watchdog means to enhance the throughput of system with the nearness of malignant hub. Watchdog serves as an interruption location scheme[13–15]

* *Author for correspondence*

for MANETs. It is in charge of identifying vindictive node in the system by indiscriminately listening to its next bounce's transmission. Moreover Watchdog plan neglects to identify pernicious conduct with the nearness of packet dropping.

ACK[16] is essentially a conclusion to end affirmation plan. The destination hub is required to send back an affirmation packet to source hub when it gets another packet.

TWOACK is a standout amongst the most vital methodologies among them. On the in opposition to numerous different plans TWOACK is neither an upgrade nor a Watchdog based plan. TWOACK identifies the acting mischievously interfaces by recognizing each information packet transmitted over each three sequential hubs along the way from source to destination. Upon the recovery of a packet, every hub along the course is required to send back an affirmation packet to the node that is two jumps far from it down the course.

SACK plan is an enhanced adaptation of TWOACK plan. The essential is to give each three back to back nodes a chance to work in a gathering to identify malevolent hub. For each three back to back nodes in the course, the third hub is required to send a SACK affirmation packet to first hub.

The center of MRA[17] plan is to verify whether the destination node has gotten the reported missing bundle through an alternate course. To start the MRA mode, the source node first ventures its nearby information base and looks for a backup way to go to the destination node. At the point when the destination node gets a MRA parcel it seeks its neighborhood knowledge base and thinks about if the reported bundle was gotten. In the event that it is as of now gotten, then it is sheltered to reason this is a false trouble making report. Generally misconduct report is trusted and acknowledged.

In Network coding method[18], instead of basically transmitting only one parcel, the mid node joins and coordinates a couple data bundle into only one bundle and after that transmits the parcel. As of late, network coding strategy has been utilized for keeping up unwavering quality as a part of MANET.

3. Proposed System

The arrangement of the proposed framework is to accomplish better packet delivery proportion in MANETS. ID based encryption has been a fundamental piece of cryptography ever. Cryptography[19–22] is the investigation of numerical procedure identified with parts of data security, for example, privacy information honesty element validation and information starting point verification. The IBE is received to guarantee the validation, uprightness and non revocation of MANETS. Considering adaptability of IBE, we watch that for a substantial number of clients, this may turn into the bottleneck. After route selection based on DSDV routing protocol[23,24] , source encrypts the data based on its public key using ID based encryption algorithm. Now only it sends the encrypted data to destination through selected neighbor nodes. Finally destination nodes decrypt the data based on its private key. Parallelly after data forwarding each node private key is updated to network and at the same time acknowledgement is updated to the source node. This was shown in the Figure 2. So identification of malicious node in the network using this algorithm is very easy and tedious.

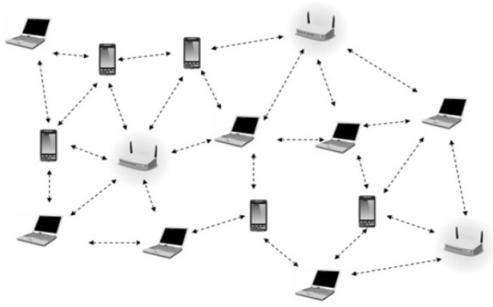

Figure 1. Mobile Ad hoc Networks.

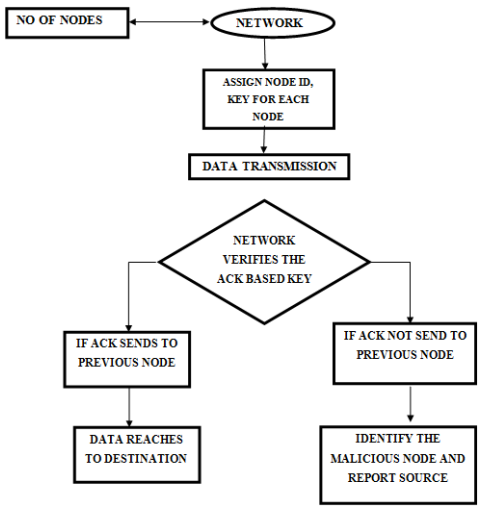

Figure 2. Proposed mechanism against packet debase in MANETS.

3.1 Algorithm

- Network deployment.
- Assign node id to each node.
- Transmit the data.
- Network verifies the key that is private key updation.
- If acknowledgement reaches the previous node means data reaches the destination.
- If acknowledgement not send to previous node means identify the malicious node.

4. Simulation Results

In a 1700x800 area arbitrarily 30 nodes are deployed. The transmission range, network area, number of sensors, packet rate, packet size, bandwidth, routing protocol, traffic type, sending and receiving slot, initial energy of sensor node, energy threshold for the network as listed in Table 1 the packet delivery proportion, throughput and end to end delivery are found using the trace files generated by ns2. In the proposed model, we increase the packet delivery proportion shown in Figure 3 and throughput shown in Figure 4 with respect to time and transmission delay is reduced, shown in Figure 5

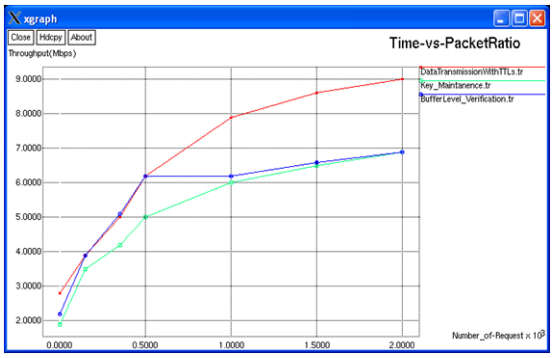

Figure 3. Packet delivery proportion vs time.

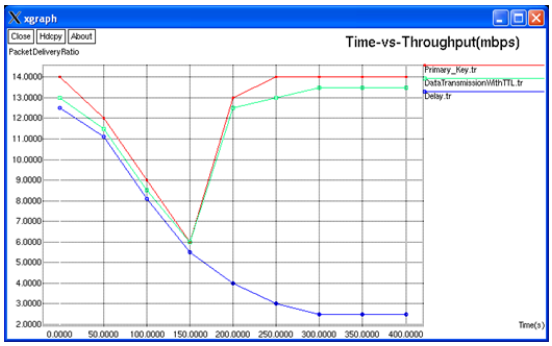

Figure 4. Throughput vs time.

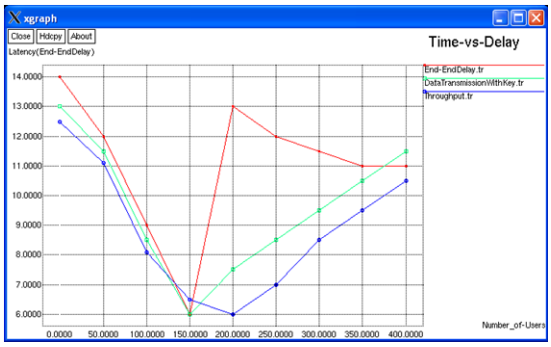

Figure 5. Transmission delay vs time.

Table 1. Simulation setup

Parameters	Value
Transmission Range	250 m
Network Area	1700 x 800
Number of Sensors	100
Packet rate	0.5 pkt/sec
Packet size	64 bytes
Bandwidth	2 Mbps
Routing Protocol	DSDV
Traffic Type	UDP
Sending and Receiving Slot	50msec
Initial energy of sensor node	100
Energy Threshold E^{thd}	3Mj

4.1 Packet Delivery Proportion

The proportion of the information bundles conveyed to the destination to those created by the sources.

4.2 Throughput

Throughput can be characterized as the quantity of parcels got effectively at sink hub over unit timeframe (as a rule a second). Throughput is measured in kbps. It can likewise be characterized as proportion of number of effectively conveyed information parcels at sink hub to the quantity of all bundles transmitted

4.3 Transmission Delay (End to End Delay)

Postponement of individual parcel is the contrast between times a bundle takes to achieve the last destination hub from starting time of a bundle from source code. In this way transmission defer (or end to end postponement) is the proportion of whole of all such defers of every parcel to the quantity of bundles transmitted from source to destination.

5. Conclusion

In the proposed protocol in this paper, node ID is assigned to each node and only after that we are transmitting the data. The network verifies private key updation for each transmission and at the same time acknowledgement is updated to the source node. So this procedure minimizes the transmission delay in the nodes. Hence packet delivery proportion and throughput is improved

6. References

1. Janevski T. 5G mobile phone concept. Proceedings of 6th IEEE Conference Consumer Communications Networking Conference; 2009. p. 823–4.
2. Ahmed A, Khan F, Rahatullah, Khan G, Ali Y. The role of mobile ad-hoc networking for pervasive computing. Int J Multi-disciplinary Sci Eng. 2012; 3(8):19–24. Available from: http://www.ijmse.org/Volume3/Issue8/paper4.pdf
3. Miorandi D, Sicari S, De Pellegrini F, Chlamtac I. Internet of things: Vision, applications and research challenges. Ad Hoc Networks. 2012; 10(7):1497–516. Available from: http://linkinghub.elsevier.com/retrieve/pii/S1570870512000674
4. Castillejo P, Martínez L, Rubio G. An internet 4 of things approach for managing smart services provided by wearable devices. Int J Distrib Sens Networks. 2013; 2013:1–9. Available from: http://www.hindawi.com/journals/ijdsn/2013/190813/
5. Prabh KS, Royo F, Tennina S, Olivares T. BANMAC: An opportunistic MAC protocol for reliable communications in body area networks. IEEE 8th International Conference on Distributed Computing Sensor System; 2012. p. 166–75. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6227738
6. Baumann R, Heimlicher S, Strasser M, Weibel A. A survey on routing metrics. TIK Rep; 2007. Available from: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:A+Survey+on+Routing+Metrics#0
7. Li P, Fang Y. On the throughput capacity of heterogeneous wireless networks. IEEE Transaction on Mobile Computers. 2012; 11(12):2073–86. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6072211
8. Akbani RH, Patel S, Jinwala DC. DoS attacks in mobile ad hoc networks: A survey. Proceedings 2nd Int Meeting ACCT; Rohtak, Haryana, India. 2012. p. 535–41.
9. Patcha A, Mishra A. Collaborative security architecture for black hole attack prevention in mobile ad hoc networks. Proceedings Radio Wireless Conference; 2003. p. 75–8.
10. Marti S, Giuli TJ, Lai K, Baker M. Mitigating routing misbehavior in mobile ad hoc networks. Proceedings 6th Annual International Conference Mobile Computer Network; Boston, MA. 2000. p. 255–65.
11. Sheltami T, Al-Roubaiey A, Shakshuki E, Mahmoud A. Video transmission enhancement in presence of misbehaving nodes inMANETs. Int J Multimedia Syst. 2009 Oct; 15(5):273–82.
12. Parker J, Undercoffer J, Pinkston J, Joshi A. On intrusion detection and response for mobile ad hoc networks. Proceedings IEEE International Conference Perform Comput Commun; 2004. p. 747–52.
13. Anantvalee T, Wu J. A survey on intrusion detection in mobile ad hoc networks. Wireless/Mobile Security. New York: Springer-Verlag; 2008.
14. Uddin M, Alsaqour R, Abdelhaq M. Intrusion detection system to detect DDoS attack in gnutella hybrid P2P Network. Indian Journal of Science and Technology. 2013 Feb; 6(2):71–83.
15. Liu K, Deng J, Varshney PK, Balakrishnan K. An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Trans Mobile Comput. 2007 May; 6(5):536–50.
16. Shakshuki EM, Kang N, Sheltami TR. EAACK a secure intrusion-detection system for MANETs. IEEE Transactions on Industrial Electronics. 2012; 60(3):1089–98.
17. Mohammadi R, Ghaffari A. Optimizing reliability through network coding in wireless multimedia sensor networks. Indian Journal of Science and Technology. 2015 May; 8(9). DOI: 10.17485/ijst/2015/v8i9/56039.
18. Menezes A, van Oorschot P, Vanstone S. Handbook of Applied Cryptography. Boca Raton, FL: CRC; 1996. p. T-37.
19. Sasi BS, Sivanandam N. A survey on cryptography using optimization algorithms in WSNs. Indian Journal of Science and Technology. 2015 Feb; 8(3). DOI: 10.17485/ijst/2015/v8i3/59585.
20. Akbani R, Korkmaz T, Raju GVS. Mobile Ad hoc Network Security. Lecture Notes in Electrical Engineering. New York: Springer-Verlag. 2012; 127:659–66.
21. Buttyan L, Hubaux JP. Security and cooperation in wireless networks. Cambridge, UK: Cambridge Univ Press; 2007 Aug.
22. Hussain MA. Deployment of mobile ad-hoc network ticket based Qos routing protocol for healthcare. Indian Journal of Science and Technology. 2015 Jul; 8(15). DOI: 10.17485/ijst/2015/v8i15/73178.
23. Ramya R, Saravanakumar G, Ravi S. MAC protocols for wireless sensor networks. Indian Journal of Science and Technology. 2015 Dec; 8(34). DOI: 10.17485/ijst/2015/v8i34/72318.