International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016 [ICSSCCET 2016]

ISBN	978-81-929866-6-1
Website	icssccet.org
Received	25 – February – 2016
Article ID	ICSSCCET063

VOL	02
eMail	icssccet@asdf.res.in
Accepted	10 - March – 2016
eAID	ICSSCCET.2016.063

Improving Security Based on Detecting Selfish Nodes Using Md5 Encryption Algorithm in MANETS

V Renupriya[1], P Priya[2] and B Gopinathan[3]

[1]Assistant Professor, Computer Science and Engineering, Karpagam Institute of Technology, Coimbatore.

[2]PG scholar, [3]Assistant Professor, Department of Computer Science and Engineering, Adhiyamaan college of Engineering, Hosur.

Abstract: *The aim of this project is to provide security mechanism for detecting selfish nodes in mobile ad-hoc network (MANET). Mobile ad-hoc network is a collection of various mobile nodes that dynamically form a network and used for communicating with each other without any network infrastructure or any centralized node. The main focus of this work is to secure the data transmission in mobile ad hoc network and this is possible by using MD5 algorithm. MANET is a self-organization network and MANET is composed of mobile nodes. In Existing system, they are taken combination of co-operate technique and collaborative technique. In co-operative technique are depended node it performs by the cost-intensive activity and some node can refuse to co-operate. Thus leading to selfish node behaviour which makes the network performance to get affected. Collaborative technique need for some kind of implementation infrastructure to maintain the accounting of detecting selfish nodes. There are many techniques are available for detecting selfish nodes. In this project, MD5 encryption algorithm, which provides security and increase the network performance.*

I. INTRODUCTION

MANETs is a mobile ad-hoc networks assume that mobile nodes voluntary co-operate in order to work properly. In MANETs nodes can freely move around while communication with each other's. Here no fixed and dedicated link available between two nodes. So any nodes can access any link between any nodes. Co-operative networking is currently receiving significant attention as an emerging network design strategy for future mobile wireless networks. Two of the basic technologies that are considered as the core for these types of networks are mobile ad-hoc(MANETs) and opportunistic and delay tolerant networks (DTNs). The co-operation on these networks is usually contact based. Mobile nodes can directly communicate with each other if a contact occurs (that is, if they are within communication range). Supporting this co-operation is a cost intensive activity for mobile nodes. Thus, in the real world, nodes couldhave a selfish behaviour, being unwilling to forward packets for others. Selfishness means that some nodes refuse to forward other nodes packets to save their own resources. A node is not forwarding the packets to the destination then their nodes are considered as the selfish nodes. The misbehaviour of selfish node, such as do not participate in routing process. The literature provides two main strategies to deal with selfish behaviour: a) Motivation or incentive based approaches, and b) Detection and exclusion. The first approach, tries to motivate nodes to activity participate in the forwarding activities. These approaches are usually based on virtual currency and/or game theory models. The detection and exclusion approach is a straight- forward way to cope with selfish nodes and several solutions have been presented. The impact of node selfishness on MANETs has been studied in it is shown that when no selfishness prevention mechanism is present, the packet delivery rates become seriously degraded, from a rate of 80 percent when the selfish node ratio is 0 to 30 percent when the selfish node ratio is 50 percent. They use watchdog technique for detecting selfish node in network. The watchdog technique is used to improve the network performance and it is based on the contact dissemination of detecting selfish nodes. The watchdog detection processes performed by can fail, it generating the false positive and false negative. Local watchdog will perform the poor performance when detecting selfish nodes, such as (DTN). The presence of colluding or malicious nodes. In this case, the effect can even be more harmful, since these nodes try to intentionally disturb the correct behaviour

Cite this article as: V Renupriya, P Priya, B Gopinathan. "Improving Security Based on Detecting Selfish Nodes Using Md5 Encryption Algorithm in MANETS". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 336-340. Print.

of the network. So in this approaches are does not providing security for detecting selfish nodes in networks. So I will introduce MD5 encryption algorithm. The MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA." MD5 is simple to implement, and provides a "fingerprint" or message digest of a message of arbitrary length.

II. Related Works

Improving selfish node detection in MANETS using a collaborative watchdog [1] In this papers watchdog are used to detect selfish nodes in computer networks. A way to reduce the detection time and to improve the accuracy of watchdog in collaborative approach. Then they introduce an analytical model to evaluate the detection time and the cost of this collaborative approach. But in these papers does not provided for detecting of selfish nodes securely.

A self-organized approach for stimulating cooperation in MANETs [2] To provide an incentive for cooperation by having a node to send its traffic at a given cost, while allowing it to profit every time it forwards others traffic. However, there are situations when a node could run out of virtual currency, and enter a broke state. In this paper, they proposed a self-organized mechanism called the broke service, which allows for a broke node to use the network to transmit its traffic, so they scheme delivers a unreasonable quality of service under a wide range of network traffic.

Assessing the vulnerability of DTN data relaying schemes to node selfishness [3] In this paper, delay tolerant networks rely on the mobility of their nodes and sequences of their contacts to transfer data. And analytically assess the performance of two popular data relaying alternatives, the unrestricted and two-hop relay schemes, when nodes behave selfishly while forwarding data. The result suggests that the performance advantage of unrestricted relaying over two-hop relaying decreases both with the number of selfish nodes and the intensity of their selfishness, irrespective of whether nodes defer from relaying deterministically or probabilistically. In this two-hop routing affected due to node selfish behaviour and routing mechanism is not better than the detecting of selfish node.

Cross Layer Approach for Selfish Node Detection in MANET [4] In this paper evaluates the AODV (Ad hoc On-demand Distance Vector routing protocol) routing protocol, there are four control messages used to establish and maintain the information and the transmission paths. These control messages include Hello message, Route Request (RREQ) message, Route Reply (RREP) message and Route Error(RERR) message. These types of control messages will process the communication in proper manner. This method will describe the degree of detecting misbehaviour nodes in ad-hoc networks. Here we are using higher-layer protocol that requires some information from the lower layer at runtime results in the creation of a new interface from the lower layer to the higher layer. In this method it does not provides better classifier of detecting selfish nodes.

Selfish Nodes Detection Using Random 2ack in MANET [5] In this paper, they introduce 2Ackschemes to detect routing Misbehaviour. This 2ACK scheme is a network layer technique in order to detect selfishness and to mitigate their effects. It can be implemented through DSR (Dynamic Source Routing) routing protocol. The 2Ack schemes are used in order to detect the misbehaviour routing through the new type of acknowledgment termed as 2Ack packets. The random 2ACK technique is based on a simple 2-hop acknowledgment packet that is sent back by the receiver to next-hop link. The 2Ack techniques take more time to detect selfish nodes, and also it will take more time to get the acknowledgement message because here there may be a packet drop.

MD5 (Message-Digest Algorithm)

MD5 algorithm is basically used to verify integrity of the data with the help of 128-bit message digest from data input. According to the standard, sometime it is called as "computationally infeasible" that any two messages that have been input to the MD5 algorithm could have as the output the same message digest, or that a false message could be created through apprehension of the message digest. MD5 is the third message digest algorithm created by Rivest. The MD5 algorithm is an extension of MD4, which the critical review found to be fast, but possibly not absolutely secure. MD5 is not quite as fast as the MD4 algorithm but it offers much more assurance of data security. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA." MD5 is simple to implement, and provides a "fingerprint" or message digest of a message of arbitrary length. Takes as input a message of arbitrary length and produces as output a 128 bit "fingerprint" or "message digest" of the input. It performs very fast on 32-bit machine.

Cite this article as: V Renupriya, P Priya, B Gopinathan. "Improving Security Based on Detecting Selfish Nodes Using Md5 Encryption Algorithm in MANETS". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 336-340. Print.

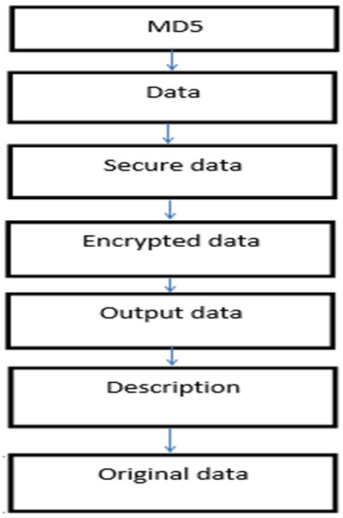

Fig 1: flow diagram of MD5

Message digest algorithm is applied to input data. Algorithm generates secure data. Secure data is divided into the encrypted data and create the output data. User sends this output data to receiver, and then on this encrypted output data receiver applied the decryption technique to get the original data.

III. Algorithm Implementation

The cooperation on mobile ad-hoc networks is usually contact based. Mobile nodes can directly communicate with each other if a contact occurs. Nodes could have a selfish behaviour, being unwilling to forward packets for others. Selfishness means that some nodes refuse to forward other nodes' packets to save their own resources.

We introduce Collaborative Contact-based Watchdog (CoCoWa) as a new scheme for detecting selfish nodes that combines local watchdog detections and the dissemination of this information on the network. Watchdog systems overhear wireless traffic and analyses it to decide whether neighbour nodes are behaving in a selfish manner. When a node detects a selfish node using its watchdog, it is marked as a positive, and if it is detected as a non-selfish node, it is marked as a negative. Even though the selfish nodes are detected they are not treated for forwarding and so going for MD5 algorithm in order to ensure the integrity of the nodes in the network.

The MD5 is an encryption algorithm used in order to ensure the integrity of the detected information carried by the nodes to the next following nodes. The malicious behaviour may happen in between the nodes on transmission of the detected information and so in order to nullify that circumstances we use MD5 encryption algorithm to ensure the integrity between the nodes and to avoid the false impersonated nodes in the network. So that the selfish nodes may not get benefit from the undertaken nodes in the network and transmission is done clearly.

IV. Methodology Description

The MD5 is an encryption algorithm used in order to ensure the integrity of the detected information carried by the nodes to the next following nodes. The malicious behaviour may happen in between the nodes on transmission of the detected information and so in order to nullify that circumstances we use MD5 encryption algorithm to ensure the integrity between the nodes and to avoid the false impersonated nodes in the network. So that the selfish nodes may not get benefit from the undertaken nodes in the network and transmission is done clearly.

MD5 Algorithm Description

MD5 algorithm consists of 5 steps:

Step 1: Appending Padding Bits. The original message is "padded" (extended) so that its length (in bits) is congruent to 448, modulo 512. The padding rules are:

Cite this article as: V Renupriya, P Priya, B Gopinathan. "Improving Security Based on Detecting Selfish Nodes Using Md5 Encryption Algorithm in MANETS". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 336-340. Print.

The original message is always padded with one bit "1" first. Then zero or more bits "0" are padded to bring the length of the message up to 64 bits less than a multiple of 512.

Step 2: Appending Length. 64 bits are appended to the end of the padded message to indicate the length of the original message in bytes. The rules of appending length are: The length of the original message in bytes is converted to its binary format of 64 bits. If overflow happens, only the low-order 64 bits are used. Break the 64-bit length into 2 words (32 bits each). The low-order word is appended first and followed by the high-order word.

Step 3: Initializing MD Buffer. MD5 algorithm requires a 128-bit buffer with a specific initial value

Step 4: Processing Message in 512-bit Blocks. This is the main step of MD 5 algorithm, which loops through the padded and appended message in blocks of 512 bits each. For each input block, 4 rounds of operations are performed with 16 operations in each round. This step can be described in the following pseudo code slightly modified from the RFC 1321's version:

Step 5: Output, the contents in buffer words A, B, C, D are returned in sequence with low-order byte first.

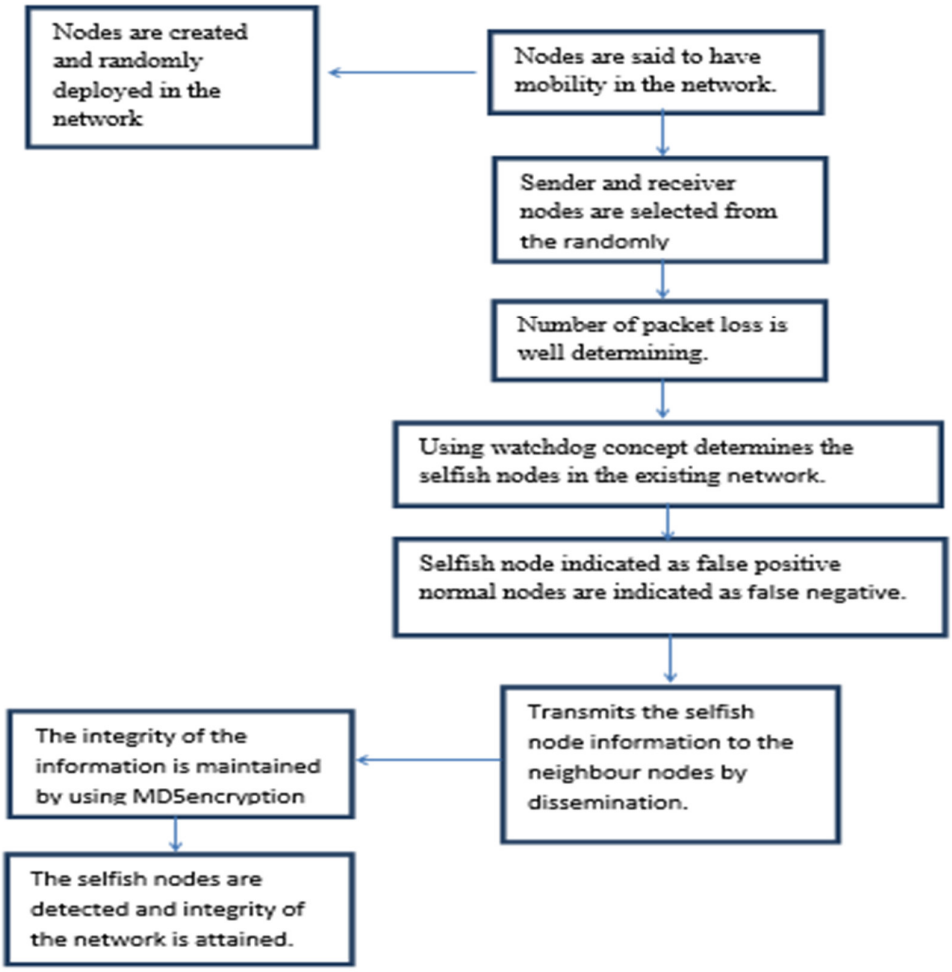

Fig 2: flow diagram of methodology description

V. Conclusion

In this paper, we have proposed Various Securities in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. Generally, MANETs suffer from various security attacks because of its features such as it provides open medium access to users. So it is very much sensitive as we consider the security issue. This study has considered the MD5 algorithm as a means of data security according to attacks. This secures the data as well as preserves the confidentiality and secure. In future, we

Cite this article as: V Renupriya, P Priya, B Gopinathan. "Improving Security Based on Detecting Selfish Nodes Using Md5 Encryption Algorithm in MANETS". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 336-340. Print.

will implement a hybrid algorithm to enhance the security in mobile ad hoc network. This hybrid algorithm consisting of Message Digest 5 & Iterative RSA algorithms and we expect the results of security enhancement to be far better.

References

1. 1.EnriqueHernandezorallo, Manuel D.Serrat, Juan-Carlos Cano" A Fast Model for Evaluating the Detection of selfish Nodes Using a Collaborative Approach in MANETs"&2012.
2. E. Hernandez-Orallo, M. D. Serrat, J.-C. Cano, C. M. T. Calafate, and P. Manzoni, "Improving selfish node detection in MANETs using a collaborative watchdog," IEEE Comm. Lett., vol. 16, no. 5, pp. 642–645, May 2012.
3. G.MurugaBoopathi, N.Insozhan, S.Vinod,"Selfish Nodes Detection Using Random 2Ack in MANETs" "International Journal of Emerging Science and Engineering" (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, February 2013.
4. Karthik m,Jyothish John, "A Survey of Techniques used to Detect selfish Nodes in MANETs in Proc.Common Technology, Feb 2013.
5. ReshmaLillMathew,Prof.P. Petchimuthu, "Detecting Selfish Nodes in MANETs using Collaborative Watchdogs" in Proc .IEEE Conf, March 2013.
6. RaduIoanCiobanu, CiprianDobre, MihaiDascalu, Stefan TrausanMatu, ValentinCristea "Collaborative Selfish Node Detection with an Incentive Mechanism for Opportunistic Networks in Proc2013 IFIP"
7. Prof. Rekha Patil, Shilpa Kallimath "Cross Layer Approach for Selfish Node Detection in MANET "International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 1, Issue 3, September 2012.
8. Karamjeet Singh, ChakshuGoel "Using MD5 AND RSA Algorithm Improve Security in MANETs Systems" International Journal of Advances in Science and Technology (IJAST) Vol 2 Issue 2 (June 2014)
9. Khushdeep Kaur1, Er. Seema 2"Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices." "International Journal of Engineering Research and Applications (IJERA)" ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 5, September- October 2012, pp.914-917.
10. Er. Mandeep SinghSandhuEr. Sunny Singla "An Approach to Enhanced Security of Multimedia Data Model Technology Based on Cloud Computing" "International Journal of Advanced Research in Computer Science and Software Engineering" Volume 3, Issue 7, July 2013.

Cite this article as: V Renupriya, P Priya, B Gopinathan. "Improving Security Based on Detecting Selfish Nodes Using Md5 Encryption Algorithm in MANETS". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 336-340. Print.