International Journal of Pure and Applied Mathematics
Volume 117 No. 15 2017, 1095-1102
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

DKGM- Device Key Generation Algorithm to Improvise Security Measures by Maintaining the Reliability Threshold in Device To Device Communication

Ms.V.M.Gayathri[1], Dr.R.Nedunchelian[2]
Research Scholar[1], Professor Department of Computer science andEngineering[2]
Saveetha University[1], Sri Venkateswara College of Engineering[2]
Vmg188@gmail.com[1], Chelian1959@gmail.com[2]

ABSTRACT:

In this modern technological world, Device-Device communication becomes an expert in all the fields. It starts from simple mobile node communication to smart sensing applications. A Mobile Ad-hoc Network is an on-demand self-forming network where nodes may either in stationary or mobile mode. Here in this network all nodes act as router. Any node can be a source or destination. Other than source and destination node are called as router nodes or intermediate nodes. Since nodes in the network may be mobile in nature, any form of nodes can involve in active participation. Absence of central node administration, results in lack of security measures. Even many application fields of MANET such as VANET etc. are prone to attacks. In this paper, we proposed an algorithm called DKGM for secure transmission of packets/data. It explains about the key generation method for initiating transmission of packets. This paper also includes maintaining the reliability of communication between two nodes. In this paper, we compare the results obtained from simulation and predicting the efficient method based on the previous and past communication details.

KEYWORD:

DGKM, MANET, VANET, Reliability, Scalability, ETV Ratio.

INTRODUCTION:

A Network is a collection of interconnected nodes for communication. A communication may be data, image, audio or video files. In this paper, we are considering data packets for communication between nodes. A network is of two types either wired or wireless. In wired network, all nodes in the network are connected through the cables. Since implementation cost is high, the entire network has been slowly changed to wireless mode. [1] Explains about MANET which is a group of nodes that may circulate freely and speak with every different using Wi-Fi gadgets. For nodes that aren't within the direct verbal exchange variety of MANET, different nodes inside the community collaborate to relay packets. A MANET is characterized by way of its dynamic topological adjustments, confined conversation bandwidth, and restricted battery power of its nodes. The community topology of a MANET can trade frequently and dramatically, considering the fact that nodes in a MANET are able to transferring collectively or randomly. The hyperlink between any two nodes can be down/up, while they circulate out/in within the transmission range of each different. A MANET may be instable due to the signal fading interference from other alerts, or the alternate of transmission energy tiers.

In this paper, we are using DKGM algorithm for efficient communication with reduced time cost. Along with, we applied a Certificate Based Scheme where a central trusted

agency provides key for source and destination. Two separate keys are generated for source and destination node for encryption and decryption and also another set of keys will be generated for router/intermediate nodes. In section II various methodologies implemented in this area were discussed. Section III explains about the routing protocol we have used for our implementation. Section IV describes the implementation methodology along with DKGM algorithm and reliability calculations. Section V shows the results obtained from various simulation strategies. Section VI includes conclusion and future reference.

LITERATURE OVERVIEW:

[2] Provides a detailed survey on various consider computing methods which can be geared in the direction of MANETs. They have specified the summary and comparisons of these tactics. In addition, they also examined various works on agree with trust propagation with trust dynamics, prediction and aggregation algorithms, they have an effect on trust dynamics and the impact of trust on safety offerings. [3] Describes about the mobility models as a survey with four sections. Initially they discussed about synthetic mobility model, next they explaining about mobile traces which have collected and analyzed, third they explained about performance degradation because of mobility issues and then finally explains about the open challenges and research area for the researchers to process.

[4] Checks the efficiency of the scheme on a modern-day station through simulation. The performance analysis suggests its suitability for massive scale MANETs. It is proven that the new scheme is provable cosy in standard version. The assessment suggests that this scheme has efficiency surpassing co generic schemes. Furthermore, a progressed scheme against chosen cipher text assault (CCA) is proposed with a view to enhance the security.

[5] Suggests a Markov-chain based totally analysis and evaluation of the OCSP-based totally certificates validations within the hybrid MANETs and the outcomes of absorbing Markov fashions are verified via the widespread simulations of the ADOPT and PS-ADOPT protocols in the OMNET++ simulator. [6] Computes direct and indirect trusting values. A certificate agency distributes keys to the nodes. A key revocation method in invoked. [7] Present a self-prepared certificate-less on-call for public key management (CLPKM) protocol, which pursuits at supplying the most powerful verification routes for authentication functions. It restricts the compromise possibility for a verification route by using proscribing its period. The different crucial issue of the protocol is that it uses a MAC characteristic rather than RSA certificate to carry out public key verifications. By doing this, the protocol saves enormous computation strength, bandwidth and storage space. The strength of the route can be verified by end to end trust value.

IMPLEMENTATION:

In this paper, we had split our work into two categories Key based communication and measuring reliability ratio. For key based communication, we proposed an algorithm called Device Key Generation Algorithm (DKGA). Reliability ratio is measured and analysed for various simulation specification. In this paper, various simulation scenarios are considered, compared and analysed for the efficient transmissions. It also further proposed to reduce the attacking strategy without degrading the performance of the network.

DKGM:

In this algorithm, we calculate trust value for each node in the network. Once calculating the trust value, one node with highest trust value will be elected as Certificate

Issue Agency/ node. The corresponding node will act as router as well as CIA according to the request. Trust node will be of any intermediate node. The information of trust node will be send to all the nodes in the network. If source node starts initiating the broadcast message it sends Source_Key_Request message to the trust node. The trust node checks the type of message and sends source_key_reply message.

A key_request message contains source_ID, destination_ID #Old_value and #value. # Value is like a unique number or a text sends by the source node for identification. the #Old_value is also a unique number which represents the previous key identification. Since it is the first request the Value for #Old_value will be null. The detination_ID will be saved in the trust node table for future confirmation. That is, when destination sends request for key it cross checks with the saved ID if it matches it generates and send it similar to the source_key_request or else it simply ignores the message.

Suppose if the trust node receives Route_request message from its neighbour node it just broadcast the message to its neighbour by updating its routing table. Based on the message, it acts promptly. When destination node receives the route_request message, it sends dest_Key_request message to the CIA node. CIA node in turn sends the dest_Key_reply message. Once the handshake messages are over the source node sends source_key_request_enc message to the CIA node where it contains the content as like as source_key_request message.

Trust value for each node is calculated based on the average taken from active participation in the network and active participation in the particular channel.

Trust value of the node in the network $TV_{Ni}=\frac{RE_i}{\cup_{j=1}^{r}\sum_{i=1}^{n}RE_i}$ ---------- (1)

Trust value of the node in the channel $TV_i=\cup_{j=1}^{r}\frac{PS_i}{PR_i}$ ---------- (2)

In the above equation (1) N represents the network and ‘i’ is the corresponding node for which we are calculating the trust value. RE represents the reliability value of that particular node to the total reliability of the entire network. In equation (2) we are calculating reliability for the dedicated channel of the corresponding node i. R represents the number of rounds for calculation. Effective Trust value is calculated based on the ratio of results of equation (1) and equation (2).

Effective Trust Value $ETV_i=\frac{TV_{Ni}}{TV_i}*100$ ---------- (3)

ETV (%)	Decision
>90	CIA node
>70 and <90	Can take as CIA node
>60 and <70	Worst condition we can allow
<60	Not allowed

Table 1. Selection of CIA node based on Effective trust value ratio

CIA node is elected based on Equation (3) value and Table (1). If two or more nodes falls on the same category, then based upon the highest value the node will be elected as CIA node. If none of the nodes fall under first category we can choose from second one. If we have node in first node then it is must to choose the respective node.

Performance measures:

Performance of the network is generally calculated based on the following factors such as scalability, reliability, energy utilization, mobility etc. In this paper, we are considering reliability, mobility and scalability issues. The output from the simulations will be analysed and necessary changes will be taken place if there is any drastic change in the networking environment.

$$\text{Reliability } AR_N = \frac{\sum_{i=1}^{k} re_{n_i}}{k} \quad \text{---------- (4)}$$

$$\text{Scalability } SC_N = \frac{\sum_{j=1}^{k}\sum_{i=1}^{n} sc_i}{k} \quad \text{---------- (5)}$$

$$\text{Trust Value Average } AT_N = \frac{\sum_{i=1}^{k} ETV_i}{k} \quad \text{---------- (6)}$$

The above equations (4), (5) and (6) are used to calculate the average values based on k number of simulations. The values obtained from the calculations are compared for the normal communication with DKGM communication between nodes.

RESULTS:

Ns2 simulator is used for our implementation. In the below table 2 we have explained about the simulator instance of our environment. The protocol we have used is AODV. The maximum simulation time we have taken is 300 sec.

Simulator Instance	
Parameters	**Default Values**
Topology	Dynamic
Number of nodes	20-100
Transmission range	100m
MAC Protocol	802.11
Network Protocol	AODV
Packet Size	512 Byte
Packet Interval	100 packet/sec
Bandwidth	5Mbps
Simulation Time	Maximum up-to 300sec

Table 2. Simulation instance for implementation

In the following results, we were calculated reliability and scalability measures and then compared with Improvised algorithm implementation.

Without DGKM reliability		**With DGKM reliability**	
Trial Number	Reliability (PDR) %	Trial Number	Reliability (PDR) %
1	67	1	89
2	65	2	87
3	88	3	92
4	43	4	79
5	24	5	67
6	77	6	97
7	53	7	84
8	63	8	76
9	36	9	84
10	40	10	91

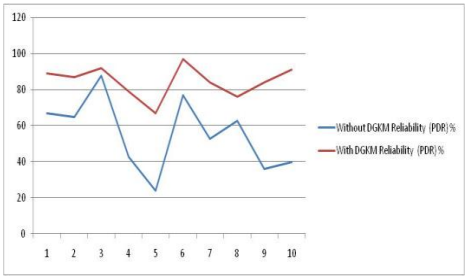

Table 3. Comparison of reliability (%) with and without using DGKM algorithm. Figure 6 Comparison of reliability (%) with and without using DGKM algorithm

In the above table 3 and figure 6 represent the Packet Delivery ratio for 10 number of trails. In the left side columns of table 3 represents the values without using DGKM algorithm and in the right hand side represents the values with using DGKM algorithm. The values marked with red colour shows the worst percentage of PDR. The worst trail form the above table 2 is 9. But if u take the results from Using DGKM algorithm only one value is below 70 other values are moderate and good.

Without DGKM scalability		**With DGKM scalability**	
Number of nodes	Reliability (PDR) %	Number of nodes	Reliability (PDR) %
20	86	20	95
45	70	45	86
34	75	34	90
78	45	78	80
90	32	90	74
65	63	65	82
27	82	27	93
44	67	44	87
86	38	86	78
73	49	73	79

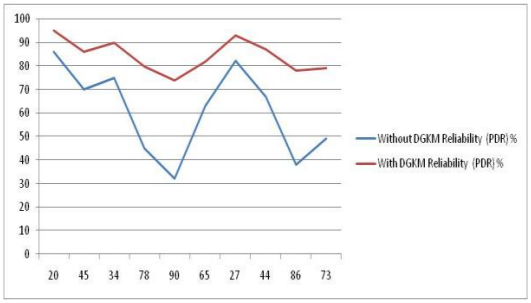

Table 4. Reliability (%) based on scalability using DGKM also compares with without using DGKM algorithm Figure 7. Reliability (%) based on scalability using DGKM also compares with without using DGKM algorithm

From the table 4 and figure 7 incurs that without using DGKM algorithm when scalability level increases it shows drastic decrease in the PDR (%). We have taken only 10 random simulation environment with different n number of nodes. But when we use DGKM algorithm the performance shows good percentage. The worst scenario is 90 nodes in the network gives 32 % pdr without using the DGKM algorithm.

Trust value calculation	
Node (for 10 nodes randomly selected)	**Effective Trust Value Ratio**
1	48
3	95
7	67
10	80
23	98
56	63
89	79
67	50

39	43
8	56

Table 5. Effective Trust Value Ratio for randomly selected nodes in the network

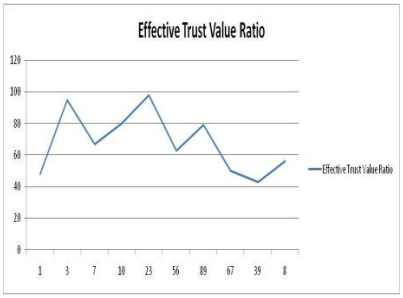

Figure 8. Effective Trust Value Ratio for randomly selected nodes in the network

In table 5 and figure 8 shows randomly selected node form 100 number of nodes at the maximum and its corresponding Effective Trust Value Ratio is measured. The values marked with red colour are cannot be participate in the communication since its value is too low. The value is highlighted with green colour has highest value which has been selected as CIA node. Suppose if two or more nodes are in the same value then by two or more trails we can select.

CONCLUSION:

In recent days, ad-hoc network becomes more and more helpful to the commercial world. The main application of MANET is vehicular network which is a prompt example for mobile communication. Although it emerges rapid growth in the field of research. Still it lags in major issues such as scalability, reliability, mobility, security etc. In this paper, we proposed a key generation algorithm called DKGM (Device key Generation Algorithm) which selects the CIA node from the network based on the highest Effective trust Value ratio. Source and destination node communicate with the CIA node before it starts transmitting the data packets. We have adopted public key cryptography method for our work. Henceforth we have used RSA key generation algorithm for generating public key and private key. This method is invoked since it is not advisable to share keys via intermediate nodes because of node's mobility. Performance evaluation is done and compared with various possibilities of simulation strategies. In future we had an idea to implement to select more than one CIA node to make the logic parallel and issues regarding mobility to be considered in detail.

REFERENCES

[1] Inderpreet Kaur , A. L. N. Rao, "A Framework to improve the Network Security with Less Mobility in MANET", International Journal of Computer Applications Volume 167 – No.10, June 2017, Pages 0975 – 8887 .

[2] Kannan Govindan, Prasant Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", IEEE Communications Surveys & Tutorials, Volume 14, Issue 2, May 2011, Pages 279 – 298.

[3] Suvadip Batabyal, Parama Bhaumik, "Mobility Models, Traces and Impact of Mobility on Opportunistic Routing Algorithms: A Survey", IEEE Communications Surveys & Tutorials, Volume 17, Issue 3, April 2015, Pages 1679 – 1707.

[4] YangYang et al, "Broadcast encryption based non-interactive key distribution in MANETs", Journal of Computer and System Sciences, Volume 80, Issue 3, May 2014, Pages 533-545.

[5] MohammadMasdari et al, "Markov chain-based evaluation of the certificate status validations in hybrid MANETs", Journal of Network and Computer Applications, Volume 80, February 2017, Pages 79-89.

[6] BanothRajkumar et al, "Trust Based Certificate Revocation for Secure Routing in MANET", Procedia Computer Science, Volume 92, 2016, Pages 431-441.

[7] SoumyadevMaity et al, "Self-organized public key management in MANETs with enhanced security and without certificate-chains", Computer Networks, Volume 65, June 2014, Pages 183-211.