Secured Cluster Based Distributed Fault Diagnosis Routing for MANET

Vani Garikipati, N Naga Malleswara Rao

Abstract*: *Mobile Ad-hoc Network (MANET) has become very crucial for many industrial applications. It is dynamic in nature. Due to its mobility and resource constrainedness and dynamic topology, MANET is vulnerable to many attacks. Therefore it is indispensable to have secure and efficient communications in MANET. Towards this end, in this paper, a novel routing approach is proposed. It is known as cluster-based distributed fault diagnosis routing which is highly secure in nature. The proposed system model includes fault diagnosis and also secure key distribution. Keeping this in mind clusters are created in MANET appropriately. The cluster-based approach in MANET is capable of distributing the aggregated data. Data in each cluster is to be distributed to respective data center. A node in the cluster that has high energy resources is considered to be cluster head. The process of secure routing in the MANET is made by defining a procedure known as pseudonymity. The proposed model is implemented using NS2 simulations.

Index Terms*: *Mobile Ad Hoc Network, Clustering, Diffie-Hellman key, pseudonym

I. INTRODUCTION

MANET is formed among devices that do not need fixed infrastructure to have a network. The nodes are self configured and the topology is dynamic in nature. The nodes are autonomous and the communication takes place using many protocols as explored in [1]. MANET supports both proactive and reactive protocols for routing. However, there are security issues to be addressed. If not, the routing process results into possibility of various attacks. The attacks may include Denial of Service (DoS), forgery, replay and so on. Clustering concept in MANET in used [2] in order to overcome such issues. There are different kinds of solutions like trust based and cluster based mechanisms. When head of a cluster is compromised, its impact will be more on the cluster. Chatterjee et al. [3] investigated a protocol known as STACRP. It stands for Secure Trusted Auction Oriented Clustering. It could provide a trusted environment in the MANET. It detects nodes that have been compromised. It also empowers the network with co-operative communication. In [4] an ID-based framework is used for MANET security. It takes care of anonymous cluster based approach and protects nodes and their data privacy. The framework uses a hybrid approach with threshold signature and pseudonym sans pairing process. Thus nodes maintain ID based anonymity. The concept of trust management in MANET is explored in [5]. When trust is considered, the block holes are avoided. With the trust scheme, it is possible to have energy efficient approach for detection of routes correctly.

In [6] residual energy based reliable multipath routing scheme (RERMRS) is proposed. The routes discovered with this are good for data transfer. They are fault tolerable in nature. The techniques used here are useful to small networks with less number of transactions. When the size of network is increased, the scheme shows its limitations. In [7] various attacks are analyzed with different security schemes. However, they are found to be computationally expensive and prone to DoS attacks. In this paper MANET attacks are analyzed and a countermeasure is proposed. It is known as Secured Cluster-based Distributed Fault Diagnosis Routing (SCDFDR). It is a protocol that supports secure communications in MANET. The proposed scheme makes MANET communications more secure in a distributed and dynamic environment. Individual node's trust and reliability is considered for making decisions. Cluster based approach with cluster functions and diagnosis of faults are considered.
The remainder of the paper is structured as follows. Section 2 presents the proposed network model. Security fault diagnosis model is presented in Section 3. The proposed protocol is presented in Section 4 while section 5 presents the evaluation results. Section 6 concludes the paper and provides directions for possible future scope of the research.

II. NETWORK MODEL

This section provides details of the proposed network model. In the model each node is supposed to store a collection of pseudonyms. However, there is no renovation of pseudonyms to reflect identities. Unique linked is used associated with pseudonyms. The pairing approach associated with Diffie-Hellman key authentication for secure communications. The interface is established with IEEE 802.11g. The same interface range is used for communication. Packets are broadcasted by Pi and the trust value Ti is configured. The function f(Ci) is used to have cluster formation as defined in Eq. 1.

$$f(C_i) = \{N_i, P_i, T_i\}. \qquad (1)$$

As per cluster formation procedure, different zones are formed in the network. The zones are denoted by x and the nodes in the zones have adhered to cluster formation function as in Eq. 2.

$$(x) = \begin{cases} \log_x X, \\ \log_x Y, \ x \geq 1. \end{cases} \qquad (2)$$

Manuscript published on 28 February 2019.
***Correspondence Author(s)**

Sri. Vani Garikapati, Research Scholar, Dept. of CSE, Acharya Nagarjuna University, Guntur, India.
Dr. N Naga Malleswara Rao, Dept. of CSE, RVR&JC College of Engineering, Guntur, India.

Network area range is determined and the logarithmic operation s is performed on the range with x, y of nodes.

III. SECURITY FAULT DIAGNOSIS MODEL

This section provides fault diagnosis model for security. The model here computes the level of security provided by a node and makes use of communication fault probability function S(q). Fault probability reflects the node's rate of interactivity and energy at different intervals. Assuming a node has many neighbor nodes. The probability interact ion is computed as follows.

$$P(q) = log_{(x,y)} N_i \tag{3}$$

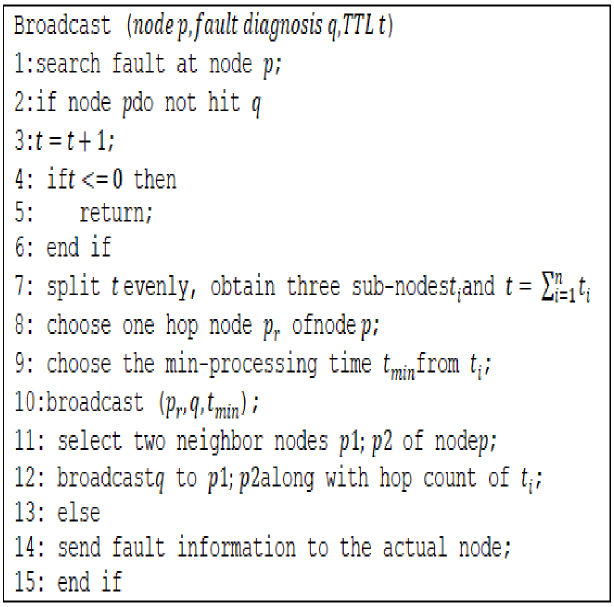
The S(q) is meant for considering both energy rate and interaction probability rate in order to have final probability rate computed at different hops of network. It is shown in Eq. 4 and Eq. 5.

$$E(q) = \int_{i=1}^{n} N_{E_i}. \tag{4}$$

$$S(q) = \{P(q), E(q)\} \tag{5}$$

A. Pseudo Code for Fault Diagnosis Model

This section provides pseudo code for the proposed fault diagnosis model.



```
Broadcast (node p, fault diagnosis q, TTL t)
search fault at node $p$;
if node $p$do not hit $q$
$t = t + 1$;
if$t <= 0$ then
    return;
end if
split $t$ evenly, obtain three sub-nodes$t_i$and $t = \sum_{i=1}^{n} t_i$
choose one hop node $p_r$ ofnode $p$;
choose the min-processing time $t_{min}$from $t_i$;
broadcast ($p_r, q, t_{min}$);
select two neighbor nodes $p1; p2$ of node$p$;
broadcast$q$ to $p1; p2$along with hop count of $t_i$;
else
send fault information to the actual node;
end if
```

As per the pseudo code, a node is able to broadcast a packet to many nodes. The packet sent includes fault diagnosis field and the time needed for processing. If any other node accepts the packet then the processing time is intentionally incremented. Thus it is repeated to all hops in the path. Minimum processing time is considered appropriate. Accordingly the flag value of fault diagnosis field changes.

IV. SECURED CLUSTER BASED DISTRIBUTED FAULT DIAGNOSIS ROUTING (SCDFDR) MODEL

This is the proposed model. It is known as Secured Cluster-based Distributed Fault Diagnosis Routing (SCDFDR) protocol which is shown in Figure 1. It has two phases. The first phase is cluster setup and the second phase is secure clustered routing scheme. The protocol uses secure ID based encryption and group signature scheme.

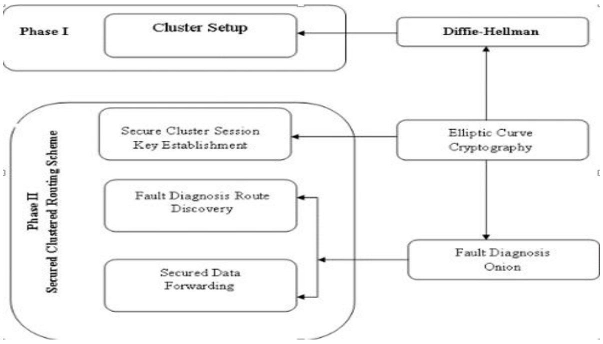

Phase I
Cluster Setup
Diffie-Hellman
Phase II
Secured Clustered Routing Scheme
Secure Cluster Session Key Establishment
Elliptic Curve Cryptography
Fault Diagnosis Route Discovery
Fault Diagnosis Onion
Secured Data Forwarding

Figure 1: Proposed scheme with overview

As presented in Figure 1, it is evident that the scheme is able to support secure data forwarding and fault diagnosis in order to provide secure communications in MANET.

A. Cluster Setup

This phase takes care of cluster formation and cluster head selection. Both are important for the functioning of the MANET. Energy efficient approach is followed to select cluster head. It is based on the residual energy for nodes. It also diagnoses faults while performing verification or measurement of parameters of cluster security. In the clustering phase a node is selected with same communication range and compatible with clustering function f(x). The nodes in a cluster communicate to cluster head denoted as CH.

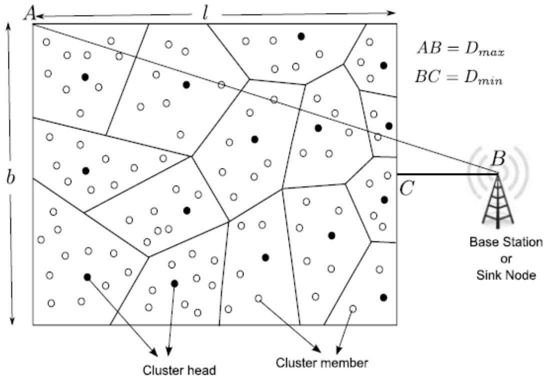


Figure 2: Cluster setup process

Secure cluster communication process is established. Cluster key is generated by CH. It makes use of Diffie-Helman scheme. The cluster key is known to all nodes in the cluster while the private key is known to cluster member node. This will help in secure communication and tracking signatures. The feature group signature is used for routing that ensures fault diagnosis. In the process encryption scheme is used that employs pseudonym. It provides complete security and does not reveal the identity of signer as well. A bilinear mapping function is used. It is denoted as$b: C_1 \times C_2 \rightarrow C_2$. It generates a tuple represented as (p, G_1, G_T, e, P). The cluster head chooses $(P_0, HG_{\in u} G_1, \gamma \in u Z_p^*)$,γ, sets $P_{pub} = \gamma P$ and $\Delta = e(P, P)$. Then an ID-based private key is generated for a given node. It is denoted as $PR_x = \gamma H(q)$ and the corresponding public key is denoted as $PU_x = (P, P_{pub}, P_0, H, \Delta)$.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

B. Secure Cluster Routing Scheme

This is the second phase in the protocol. In this phase session key is established. Secure route discovery is carried out. Session is creation is as explored in [12] and [13]. It makes use of fault diagnosis routing scheme as mentioned earlier. The nodes in the MANET broadcast route request packet in order to achieve discovery of routes. The request dented RREQ has fault error rate flag as well. Once a route is formed without faults, the secure data transmission is ensured between source and destination nodes. In the routing phase, the nodes broadcast packets to neighbor in the same communication zone. This process is illustrated in Figure 3. Route information as explored in [11] is used in this process as well.

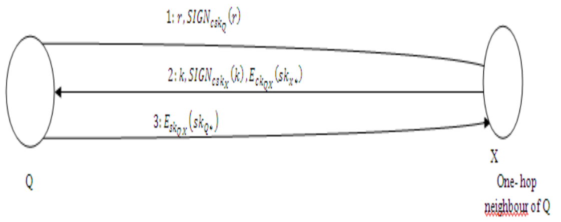
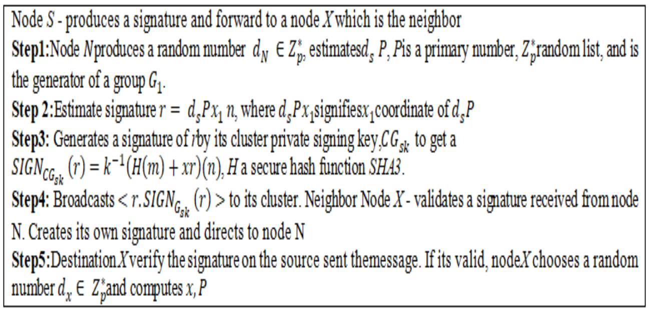

$1: r, SIGN_{csk_Q}(r)$
$2: k, SIGN_{csk_X}(k), E_{ck_{QX}}(sk_{X*})$
$3: E_{sk_{QX}}(sk_{Q*})$
X
Q
One- hop
neighbour of Q

Figure 3: Secure Cluster Session Key Establishment

The following is the procedure used for establishing secure cluster session key which is crucial for communications in MANET.


Node S - produces a signature and forward to a node X which is the neighbor

Step1: Node N produces a random number $d_N \in Z_p^*$, estimates $d_s\ P$, P is a primary number, Z_p^* random list, and is the generator of a group G_1.

Step 2: Estimate signature $r = d_s P x_1\ n$, where $d_s P x_1$ signifies x_1 coordinate of $d_s P$

Step3: Generates a signature of r by its cluster private signing key, CG_{sk} to get a $SIGN_{CG_{sk}}(r) = k^{-1}(H(m) + xr)(n)$, H a secure hash function $SHA3$.

Step4: Broadcasts $< r.SIGN_{G_{sk}}(r) >$ to its cluster. Neighbor Node X - validates a signature received from node N. Creates its own signature and directs to node N

Step5: Destination X verify the signature on the source sent themessage. If its valid, node X chooses a random number $d_x \in Z_p^*$ and computes x, P

The procedure as provided here makes use of Elliptic Curve Diffie-Hellman (ECDH) as explored in [8] and the Elliptic Curve Digital Signature Algorithm (ECDSA) as studied in [9]. This combination makes it more effective in secure and authentication as well.

C. Fault Diagnosis Route Discovery

This section provides fault diagnosis route discovery. Session key is initialized and the fault diagnosis is made with probability. The actual process makes use of a collection of secure cluster route requests and the corresponding secure cluster route replay packets. This process is illustrated in Figure 4. The route discovery process is initiated by route request packet and the process is denoted as in Eq. 6.

$$\langle SCREQ, S(Q), seqno, C_{dest} \rangle \qquad (6)$$

The variables seqno, *SCREQ* and C_{dest} denote the packet sequence number secure cluster route request packet and the member of destination in a cluster. One way has function is used for collision resistance. The digest related value is denoted as X. The process related to fault diagnosis is named as Trapdoor Boomerang Fault Diagnosis ($K_{commit}(D)$).

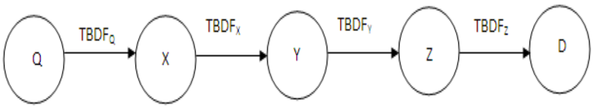


Figure 4: Fault Diagnosis Route Discovery

$$TBDF_S = E_{\overline{sk}_{Q*}}(Q)$$

$$TBDF_X = E_{\overline{sk}_{X*}}\left(Nonce_X, E_{\overline{sk}_{Q*}}(Q)\right) \qquad (8)$$

$$TBDF_Y = E_{\overline{sk}_{Y*}}\left(Nonce_Y, E_{\overline{sk}_{X*}}\left(Nonce_X, E_{\overline{sk}_{Q*}}(Q)\right)\right)$$

(9)

$$TBDF_Z = E_{\overline{sk}_{Z*}}\left(Nonce_Z, E_{\overline{sk}_{Y*}}\left(Nonce_Y, E_{\overline{sk}_{X*}}\left(Nonce_X, E_{\overline{sk}_{Q*}}(Q)\right)\right)\right)$$

(10)

After receiving RREQ from the source node, the neighbor is able to validate the source. In addition to this there is verification of trapdoor information. The sequence number of routing packet and the encrypted source id and also verified. Other fields considered in the process include hp count and flow id. X forwards SCREQ PACKET in order to have boomerang fault diagnosis. Finally SCREQ is transmitted to other nodes in order to have secure communication. Once there is acknowledgement on SCREQ, the RREQ is sent to destination node. The neighbor node is bale to verify destination node by using trapdoor details using pseudonym-based key. Once it is identified as valid destination node, the information is updated to the source node. Accordingly there will be route replay. If there are multiple route requests accepted by destination node, it gives reply to first accepted packet. After its validation is found true, it drops other request packets. This is done to minimize overhead.

D. Secure Cluster Route Reply

Once the destination is diagnosed and route is discovered, the destination node broadcasts a response denoted as RREP to the source with the parameters shown in Eq. 11.

$$\langle SCREP, Rnym, \{sk_{ij}\}, (pr_{dest}, TBDF) \rangle \qquad (11)$$

Here the TBDF is as mentioned earlier. Random route pseudonym is denoted as *Rnym* and secure cluster route reply is denoted as *SCREP*. Cluster session keys are denoted as sk_{ij} and the distribution keys are denoted as $sk_{zd}, sk_{yz}, sk_{xy}, sk_{qx}$ etc., pr_{dest}. The secure cluster route reply process is illustrated in Figure 5.

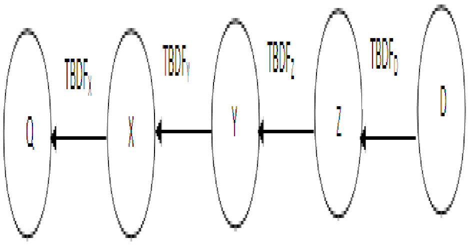


Figure 5: Secure Cluster Route Reply

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

$$TBDF_D = E_{\overline{sk}_{ZD}}\left(Nonce_Z, E_{\overline{sk}_{Y*}}\left(Nonce_Y, E_{\overline{sk}_{X*}}\left(Nonce_X, E_{\overline{sk}_{Q*}}(Q)\right)\right)\right) \quad (12)$$

$$TBDF_Y = E_{\overline{sk}_{YZ}}\left(Nonce_Y, E_{\overline{sk}_{X*}}\left(Nonce_X, E_{\overline{sk}_{Q*}}(Q)\right)\right) \quad (13)$$

$$TBDF_Z = E_{\overline{sk}_{XY}}\left(Nonce_X, E_{\overline{sk}_{Q*}}(Q)\right) \quad (14)$$

$$TBDF_X = E_{\overline{sk}_{QX}}(Q) \quad (15)$$

SCREP packet is sent from destination node to other node. Once it is received, the other node takes car e of validation and fault diagnosis using boomerang approach. In the process the cluster session key is also used. The entire procedure is illustrated in Figure 4 and Figure 5. The verification is notified to the destination node. There is an alternative concept known as alternative random route pseudonym in order to study the fault diagnosis process. In the process, the new pseudonym is updated and the route discovery table is correctly mapped. This process is repeated by all other forwarding nodes associated with their session keys. When fault free nodes are found, the source node is able to accept packets and communication with the destination node will be successful.

E. Secure Cluster Data Forwarding

After validation of the route that has been discovered, it generates unique route pseudonym. In addition to this an exceptional route pseudonym is also setup between the source and destination nodes in the path. This establishment is required to enable secure data forwarding process. In the process, the source node is able to encapsulate packets and send them to discovered routes and then the route pseudonym information is updated into the table which has route discovery information. A lookup process is involved to take routes in the table and validate the same. If a node is found unavailable or compromised, the previous node performs change operation affecting route pseudonym and update the table in order to broadcast locally. This process is repeated till the packet reaches the desired destination. The format of packet is as follows.

$$\langle\, Rnym, sk_{ij}(TData, E_{pu}(ED))\,\rangle \quad (16)$$

The packet type is denoted as *Rnym*, *TData* while the encrypted data is represented as ED. The secure data flow is illustrated between the source and destination nodes in Figure 4.6.

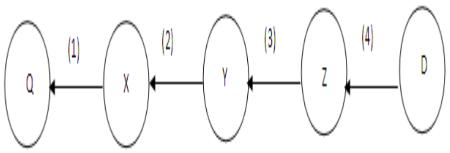


Figure 6: Secured Cluster Data Forwarding

$$(1): Rnym_{QX}, E_{sk_{QX}}\left(TData, E_{PU_D}(ED)\right) \quad (17)$$

$$(2): Rnymco_{XY}, E_{sk_{XY}}\left(TData, E_{PU_D}(ED)\right) \quad (18)$$

$$(3): Rnym_{YZ}, E_{sk_{YZ}}\left(TData, E_{PU_D}(ED)\right) \quad (19)$$

$$(4): Rnym_{ZD}, E_{sk_{ZD}}\left(TData, E_{PU_D}(ED)\right) \quad (20)$$

V. PERFORMANCE EVOLUTION

The performance of the proposed SCDFDR scheme is evaluated in this section. Then it is compared with the scheme in [15] named as SOKMTC. The performance metrics used are average end to end delay, energy consumption, and packet drop and average packet delivery ratio. The SCDFDR protocol is evaluated with NS2 [14] simulations. The simulation environment is as shown in Table 1.

Table 1: Shows environment used in simulations

Number of mobile Nodes	50 nodes
Network Area	1000 X 1000
MAC	802.11
Routing protocol	SCDFDR
Communication Radius	250m
Total Simulation Time	10 secs
Traffic Model	CBR
Data size	512
Rx Power	0.4J
Tx power	0.7J
Idle Power	0.04J
Primary Energy	10J
Data Rate	5,10,15,20 and 25Kbps

From Table 1, it is understood that the number of mobile nodes considered for simulation are 50. The traffic model used is CBR. The network area is 1000m x 1000m. The mobility considered is 5m/s. The cluster function f(c) is used to form clusters and then the energy model is used to have cluster head selection.

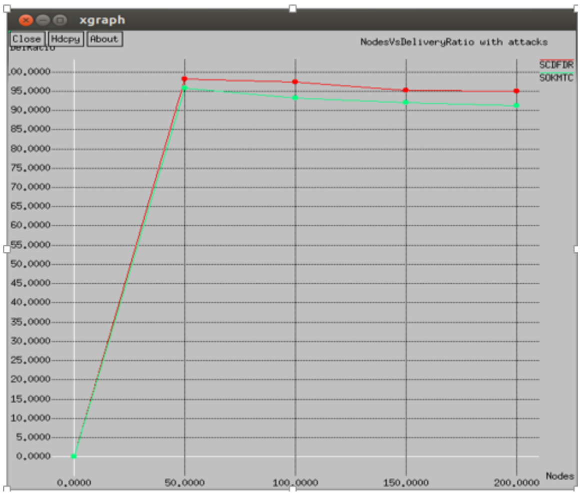


Figure 7: Packet delivery ratio

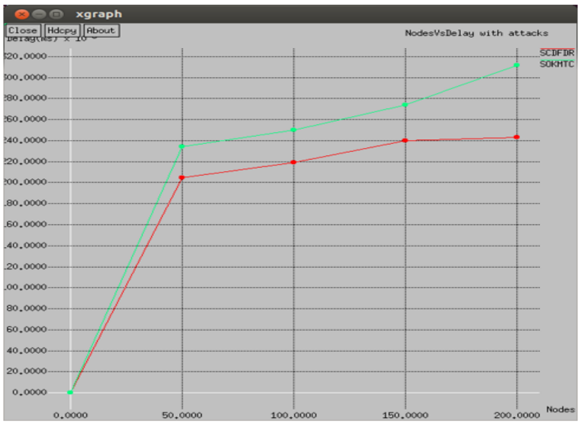


Figure 8: End-to-End delay

As shown in Figure 7 and Figure 8, the packet delivery ratio and end to end delay are evaluated respectively. The comparison is made between the proposed protocol and the existing work found in [15]. The proposed method is found better than the existing.

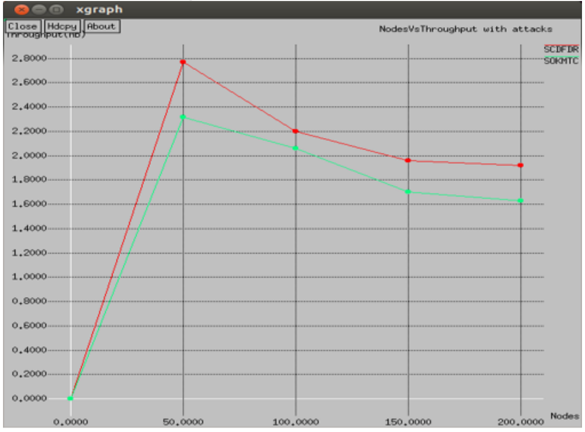


Figure 9: Throughput vs Number of nodes

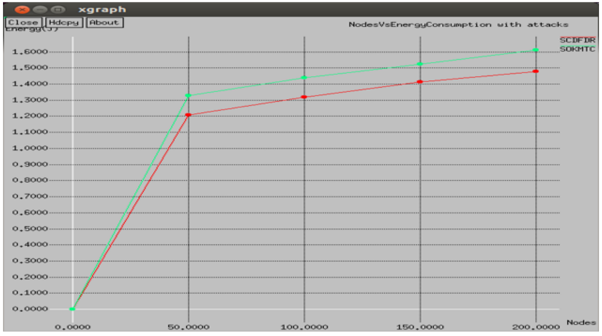


Figure 10: Energy Consumption

As shown in Figure 9, it is evident that the throughput of the SCDFDR is better than that of SOKMTC. There is performance difference between them. There is up to 15% increase in the performance of throughput. It reflects the efficiency of the proposed method. Similarly Figure 10 shows the performance of the schemes in terms of energy consumption. The energy consumption of the proposed system is less than that of the existing one. There is 8% less consumption of energy is exhibited by the proposed scheme.

VI. CONCLUSION

In this paper, we proposed a routing protocol in MANET for efficiency in communications. It is known as cluster-based distributed fault diagnosis routing protocol. In order to complete the protocol, the process is divided into two parts. In the first part two aspects are carried out. They are known as formation of clusters and key management. With these two aspects cluster setup and key management is achieved. In the second phase of the protocol, fault diagnosis routing and pseudonymity are considered. It diagnoses failures and find malicious nodes that reduce problems in distributed communications. Once the network discovery is completed, secure data transmission is in place with unique pseudonym routes in order to minimize routing failures. The proposed model is evaluated using NS2 simulations. The empirical results revealed that the system is capable of providing secure transmissions in distributed environment. The system is able to prevent attacks besides reducing energy consumption. In future we intend to perform more experiments in terms of different kinds of attacks and improve the model.

REFERENCES

1. A.A. Abbasi and M. Younis. "A Survey on Clustering Algorithms for Wireless Sensor Networks."Volume 30, Issues 14–15, 15 October 2007.
2. C. Tselikis, S. Mitropoulos, N. Komninos, and C. Douligeris. "Degree-based clustering algorithms for wireless Ad Hoc networks under attack." IEEE Communications Letters, vol. 16, no. 5, pp. 619–621, 2012.
3. P. Chatterjee, I. Sengupta, and S. K. Ghosh, "STACRP: a secure trusted auction oriented clustering based routing protocol for MANET," Cluster Computing, vol. 15, pp. 303–320, 2012.
4. YoHan Park, YoungHo Park and SangJae Moon, "Anonymous Cluster-Based MANETs with Threshold Signature", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013, Article ID 374713.
5. Yuxin Liu, Mianxiong Dong, Member, IEEE, Kaoru Ota, Member, IEEE, Anfeng Liu, "Secure and Trustable Routing in Wireless Sensor Networks", IEEE Transactions 1556-6013 (c) pp. 1-14, 2016.
6. Prof. N. Sureshkumar and Dr. S.Bhavani "Residual Energy based Reliable Multipath Routing Scheme for increasing Network Lifetime in MANET" International Journal of Applied Engineering Research ISSN 0973-4562 pp. 1908-1913 Volume 12, Number 9 (2017) © Research India Publications.
7. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2-3), 293-315.
8. R. J. Ik, O. K. Jeong, and H. L. Dang. "A Diffie-Hellman Key Exchange Protocol without Random Oracles." in Proc. 5th International Conference on Cryptology and Network Security, Springer-Verlag Berlin, pp. 37-54, 2006.
9. D. Johnson, and A. Menezes. "The Elliptic Curve Digital Signature Algorithm (ECDSA)." Technical Report CORR 99-34, Centre for Applied Cryptographic Research (CACR), University of Waterloo, 1999.
10. Saju PJohn and PhilipSamuel. "Self-organized key management with trusted certificate exchange in MANET." https://doi.org/10.1016/j.asej.2014.09.011
11. J. Ibriq, I. Mahgoub. "HIKES:hierarchical key establishment scheme for wireless sensor networks." Int J Commun Syst (8 November) (2012), 10.1002/dac.2438.
12. Nilesh Goriya, Indr Jeet Rajput, Mihir Mehta"Low Control Overhead for Cluster Maintenance in Wireless Network for DSR Protocol." COMPUSOFT, An international journal of advanced computer technology, 4 (5), May-2015 (Volume-IV, Issue-V)
13. Milan KumarDholey,G.P.Biswas. "Proposal to Provide Security in MANET's DSRRouting Protocol."https://doi.org/10.1016/j.procs.2015.04.117
14. Network simulator https://www.isi.edu/nsnam/ns/
15. Saju P John a, *, Philip Samuel. (2015). Self-organized key management with trusted certificate exchange in MANET, Ain Shams Engineering Journal (2015) 6, 161–170.

*Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.*