A New Highly Secure and Efficient Routing Algorithm for Wireless Sensor Network

Rekha R
PG Student
JNNCE, Shimoga.

Sowmya G.V
Internal Guide
JNNCE, Shimoga

ABSTRACT
In today's world the security vulnerabilities are increasing day by day. It is really difficult to route the packet with minimum packet loss with less power consumption and high energy efficiency. In this paper a new routing protocol is presented which would route the packets in a highly efficient way by introducing the concept of friend list, unauthenticated list and question mark list. The algorithm will avoid the malicious node by studying the network in an intelligent way. The algorithm works by sending challenges and sharing friend list to provide a list of trusted nodes to the source node through which data is transmitted [1]. The proposed algorithm is also compared with the existing algorithms namely Trust-Based Multipath Routing (TMR), Disjoint Multipath Routing (DMR). Message Trust-Based Multipath Routing(MTMR) and the performance analysis proves that the proposed method will have better performance with respect to number of hops, route discovery time, power consumed, energy efficiency and packet loss.

Keywords
FACES scheme, friend-based Ad Hoc Routing, MANETs, Friend-list, unauthenticated-list, security of communication systems, simulation analysis

1. DISJOINT MULTIPATH ROUTING (DMR)
In this algorithm multiple routes are discovered from source to destination using Dynamic Source Routing (DSR) algorithm [2]. The routes are arranged in ascending order of the route discovery time and best possible four routes' is chosen among them. Each packet is sent, over independent routes from source to destination.

2. TRUST-BASED MULTIPATH ROUTING (TMR)

TMR provides a method of message security using trust based multipath routing [3]. In this approach, less trusted nodes are not given the encrypted parts of a message, thereby making it difficult for malicious nodes to gain access to the minimum information required to break through the encryption strategy. Using trust levels, it makes multipath routing flexible enough to be usable in networks with "vital" nodes and absence of necessary redundancy. In addition, using trust levels, it avoids the non trusted nodes in the routes that may use brute force attacks and may decrypt [4] messages if enough parts of the message are available to them.

3. MTMR ROUTING ALGORITHM

MTMR is assigned a trust assignment and updating strategy which can be used to identify and isolate malicious nodes without being hard on the resources of the network. This is the trust requirement of a particular message, which decides how the message will be routed. Therefore, only paths with certain trust level can be used for its forwarding. This further enhances the security of the system. Initially, each node is given a trust value of zero which indicates unknown trust level. Later this value may be incremented or decremented based on the behavior of the node. The Trust Level [5] would be varying in the range of $-4<T<4$. The trust levels have a range of values from -4 for minimum trust and 4 for maximum trust. Unlike TMR MTMR routing algorithm does not assign random trust levels [6] instead the trust levels are assigned only to those nodes which behave properly and deliver the packets successfully.

4. FRIEND BASED ROUTING PROTOCOL

The new routing algorithm will make use of following parameters.

Question Mark List (QML): The list of nodes which are deemed suspicious by a particular node. This list is stored for each and every node in its data structure.

Unauthenticated List (UL): The list of nodes of which no security information is present.

Friend List (FL): This is the list of nodes which convey trust. Like the question mark list, a friend list is also stored for each node in its data structure. Friends are rated on a scale of 0 to 10.

FREQ: Friend Sharing Request, this is a control packet which is used to initiate friend sharing. A node receiving this packet replies with the nodes in its friend list, unauthenticated list and the question mark list.

DR: Data Rating, this is the rating given to nodes after they transmit some amount of data for the source node.

FR: Friend Rating, this is the rating computed when nodes share their friend lists.

NR: Net Rating, this rating is computed as a weighted mean of DR and FR.

OR: Obtained Rating, rating received during the friend sharing stage.

4.1. Share Friend Stage Algorithm

This is the stage in which a node will exchange the friend list with other node in the network. The following table gives brief information about the share friend stage for various cases between two nodes namely A and B [7]

Table1. Share Friend various Stages

Friend Initiator Node A	Friend Giver Node B	Description
FL of Node A is Empty	FL of Node B is Empty UL of Node B is Not Empty	1) The Node A sends a FREQ Request to Node 2) The Node B sends a UL to Node A 3) Node A will put the nodes of UL from Node B by removing the nodes which behave maliciously 4) Node A will assign DR,FR and NR to nodes and put it in FL
FL of Node A is Not Empty	FL of Node B is not Empty	1) The Node A sends a FREQ Request to Node B 2) The Node B sends a FL to Node A 3) Node A will now find out the common nodes in both the FL's Node A will then give the Obtained Rating (OR) for FR,DR,NR and for the remaining nodes which are not common will increment the FR,DR and NR

4.2 Form Unauthenticated List

The nodes will find out the nodes in the transmission range and then it maintains a set of nodes which are reachable by the nodes on its own.

4.3. Friend Routing Protocol

The Friend routing protocol will perform the following steps

1. The Source Node will first find the set of intermediate nodes by doing a lookup in its Friend List.

2. If the friend list is empty then the source node will look into the unauthenticated List.

3. If the unauthenticated list is empty the friend list has no other choice of picking the node from question mark list.

4. The source node will check whether it contains the destination node in its list if yes then the faces protocol will transmit the data directly to the intermediate node.

5. The intermediate node will then become the source node (picked up during either the steps 1 2 and 3).

6. The process repeats until the Time to Live period expires or destination node is reached.

7. If the TTL =0 [8] then the current node will always pick a node which is closer to destination so that the destination can be reached at a faster rate.

5. RESULTS

Table2: Input to Routing Algorithms

Source Node	Destination Node	Coverage Area
5	45	30

5.1 DMR Algorithm Output

Output of Stage1 for DMR Algorithm

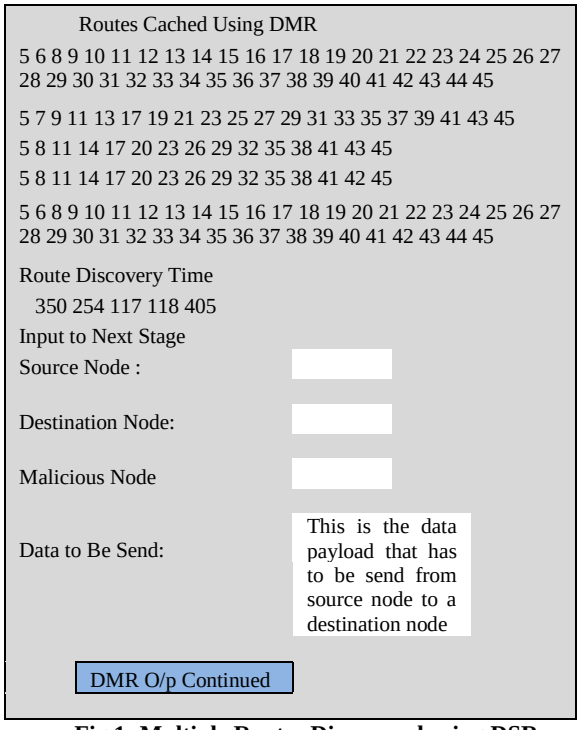

Fig 1: Multiple Routes Discovered using DSR

Fig 1 shows the multiple routes that have been discovered from source node to a destination node using DSR (Dynamic Source Routing) algorithm and there corresponding Route Discovery [9] time as well. The user is also entering the data payload that has to be sent from source node to destination node.

Output of DMR Algorithm

Table 3: Routes Chosen by DMR

Routes used by DMR Route	Time
[5,8,11,14,17,20,23, 25,29,32,35,38,41 43,45]	117
[5,8,11,14,17, 20,23,25, 29,32,35,38,41,42,45]	118
[5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35, 37,39,41,43,45]	254
[5,6,8,9,10,11,12,13,14,15,16,17,18,19,20,21, 22,23, 24, 25,26,27,28,29, 30,31,32,33,34,35, 36,37, 38,39,40,41,42,43,44,45]	350

Table 3 shows the multiple routes that are discovered using DMR algorithm [10] from source node to the destination node which have the less route discovery time.

Table 4: Packet Formation Output

PACKETS			
Packet 1 : 5	45	This is the data pay	1
Packet 2 : 5	45	load th	2
Packet 3 : 5	45	At has to be s	3
Packet 4 : 5	45	End from source node to a destination node	4
ENCRIPTED PACKETS			
Encrypted Packet 1	5	45 [B@11cd402 1	
Encrypted Packet 2	5	45 [B@1cd2ec05 2	
Encrypted Packet 3	5	45 [B@158dc 3	
Encrypted Packet 4	5	45 [B@17d03c5 4	

Table 4 shows the Packet Formed using the Triple Des Encryption [11] for the data fragments. These data fragments would be sent over multiple independent routes from source node to destination node.

5.2 TMR Algorithm Output

Table 5: TMR Algorithm Output

Trust Level	Route
0	**5 8 11 14 17 20 23 26 29 32 35 38 41 42 45**
-2	**5 6 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45**
-1	**5 8 11 14 17 20 23 26 29 32 35 38 41 42 45**

Best Route of TMR
5 8 11 14 17 20 23 26 29 32 35 38 41 42 45
Trust Level. 0

Table 5 shows the TMR algorithm having multiple routes from source node to the destination node. The TMR algorithm [12] will choose a route which is having the maximum Trust from Source Node to Destination node in the network.

5.3 MTMR Algorithm Output

MTMR Routing Algorithm [13] takes an additional parameter as input i.e. threshold trust of a route. Threshold Trust=40

Table 6: MTMR Algorithm Output

Route Using MTMR AND TRUST MAP		
TRUST 152	ROUTE	[5,6,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45
TRUST 77	ROUTE	[5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45]
TRUST 56	ROUTE	[5,8,11,14,17,20,23,26,29,32,35,38,41,42,45]
TRUST 60	ROUTE	[5,8,11,14,17,20,23,26,29,32,35,38,41,42,45]
Best Route Possible At this Time		
5,6,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44, 45		
POSSIBLE TRUST LEVEL 152		
Route Using MTMR 5 6 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 TRUST LEVEL Using MTMR 152		

Table 6 shows the MTMR algorithm having multiple routes from source node to the destination node. The MTMR algorithm will choose a route which is having the maximum Trust from Source Node to Destination node in the network. The additional thing happening in MTMR is the nodes which are in the best route will have their corresponding trust levels incremented by a factor of 1.

5.4 Friend routing algorithm output

The Friend will also take TTL has an additional input parameter as compared to other algorithms.

Table 7 shows the Friend Based Routing Algorithm output. The Friend Routing Protocol has discovered the all the routes by picking based on combination of friend rating, data rating [14] and net rating. The Friend Routing has chosen the route which is having the maximum rating as the best route.

Table 7: Friend Routing Algorithm Output

Net Rating	Route
118.0	5 5 8 11 14 17 20 23 26 29 32 35 38 41 44 45
106.0	5 5 8 11 14 17 20 23 26 29 32 35 38 41 44 45
124.0	5 5 8 11 14 17 20 23 26 29 32 35 38 41 44 45
112.0	5 5 8 11 14 17 20 23 26 29 32 35 38 41 44 45
Best Route Discovered and Rating 5 5 11 14 17 20 23 26 29 32 35 38 41	
44 45 Rating Route 124.0 5	

Table 8 shows the output of Friend Sharing Stage As seen in the figure the friend list of Friend Stage Initiator is shown where the Node Id are friend node ids , Friend Rating from giver is rating allocated from node 5. Friend Rating from initiator is as per node 4. Similarly Data Rating and Net Rating are shared between two nodes Node 4 and Node5.

Table 8: Friend Sharing Stage Output

NodeId	Friend Rating From Giver	Friend Rating From Initiator	Data Rating From Giver	Data Rating From Initiator	Net Rating From Giver	Net Rating From Initiator
6	1	1	1	1	1	1
9	1	1	1	1	1	1
12	3	3	3	3	6	6
32	4	0	3	0	6	0
35	4	4	3	3	6	6
38	4	0	3	0	6	0
45	4	0	3	0	6	0
41	4	0	3	0	6	0
44	4	0	3	0	6	0
30	10	10	11	11	65	0
25	10	18	11	19	65	65
26	10	10	15	11	108	101
29	10	10	15	11	108	65
23	10	10	27	23	270	211
20	10	10	27	23	270	211
17	10	10	27	23	270	211
14	10	10	27	23	270	211
11	10	10	29	25	302	240
8	10	10	29	25	302	240
5	10	10	41	33	520	369

6. Simulation Analysis of Algorithms

6.1 Number of hops

Fig 2 shows the number of hops taken from source to destination for all four algorithms DMR, TMR, MTMR and FACES (Friend Algorithm).As seen from figure FACES has least no. of hops

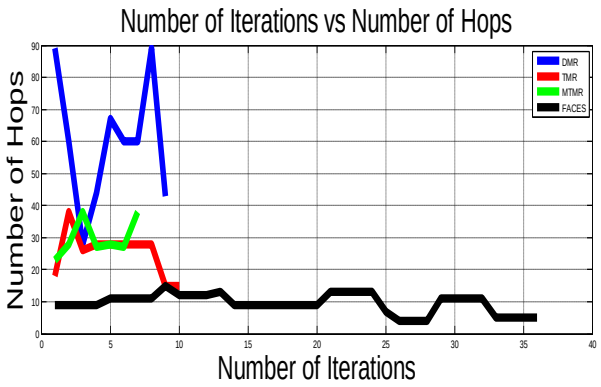

Fig 2: No. of Hops Comparison

6.2. Route Discovery Time

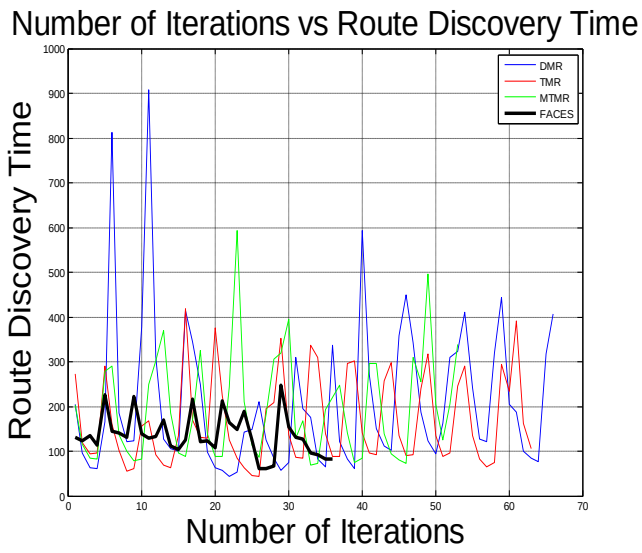

Fig 3: Route Discovery Time

Fig 3 shows that the route discovery time taken by FACES algorithm is less as compared to DMR, TMR and MTMR.

6.3 Packet Loss

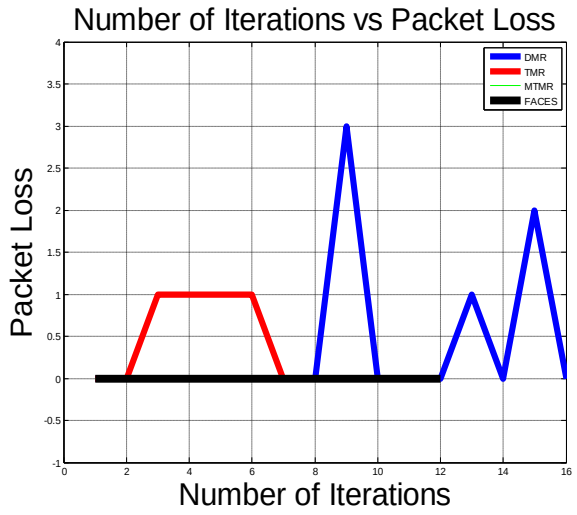

Fig 4: Packet Loss

Fig 4 shows that Packet Loss in the case of FACES is less as compared to TMR, MTMR, and DMR

6.4 Power Consumed

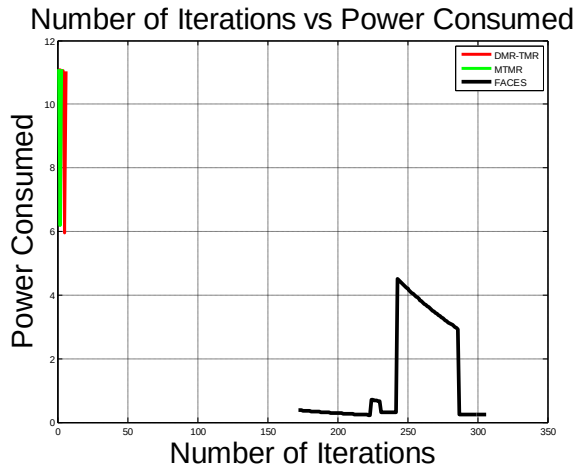

Fig 5: Power Consumed

Fig 5 shows that Power Consumed during the route discovery mechanism in faces in the case of FACES is less as compared to TMR, MTMR, and DMR

6.5:EnergyEfficiency

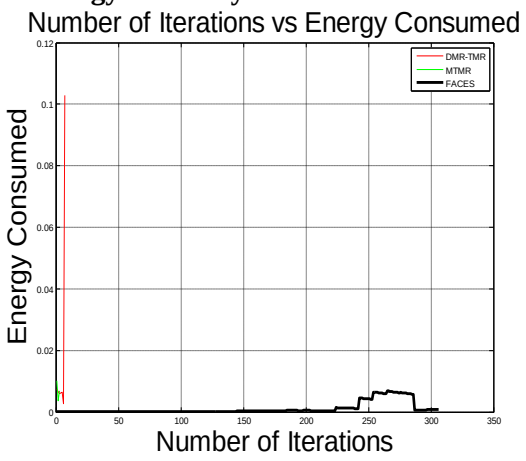

Fig 6: Energy Consumed

Fig 6 shows that the Energy consumed in case of FACES is the least as compared to other algorithms.

7. CONCLUSION

Many Routing algorithms namely DMR, TMR, MTMR and Friend (FACES) have their own way in order to establish the trust and transmit packet securely. Friend based protocol proved to be best in terms of no of hops, route discovery time, packet loss, power consumed and energy consumed.

7.1 Future Scope

7.1.1 The Routing Algorithm must being mature by not maintaining the malicious node in the question mark list. The malicious node should be completely dismantled from the entire network.

7.1.2 The maintenance overhead of the faces routing algorithm must be completely reduced because there is an overhead on each node in order to maintain the routing tables, question mark list, friend list and unauthenticated list.

8. REFERENCES

[1] L.Wang and N.-T. Zhang, "Locally forwarding management in ad-hoc networks," in *Proc. IEEE Int. Conf. Communications, Circuits and Systems and West Sino Expositions*, Jun./Jul. 2002, pp. 160–164.

[2] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Book Chapter inMobile Computing*, T. Imielinski andH. Korth, Eds. Dordrecht, The Netherlands: Kluwer, 1996, pp. 131–181.

[3] A. Wood and J. A. Stankovic, "A taxonomy for denial-of-service attacks in wireless sensor networks," in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*. Boca Raton, FL: CRC, 2005, pp. 32:1–32:20.

[4] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

[5] M. S. Obaidat and N. Boudriga, *Security of e-Systems and Computer Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2007.

[6] K. Sanzgiri, B. N. Levine, C. Shields, B. Dahill, and E. M. Belding- Royer, "A secure routing protocol for ad hoc networks," in *Proc. 10th IEEE Int. Conf. Network*.

[7] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

[8] M. S. Obaidat and N. Boudriga, *Security of e-Systems and Computer Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2007.

[9] K. Sanzgiri, B. N. Levine, C. Shields, B. Dahill, and E. M. Belding- Royer, "A secure routing protocol for ad hoc networks," in *Proc. 10th IEEE Int. Conf. Network Protocols (ICNP)*, Paris, France, Nov. 12–15, 2002, pp. 78–89.

[10] Y. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks,"*Wireless Netw.*, vol. 11, no. 1–2, pp. 21–38, Jan. 2005.

[11] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in *Proc. MobiCom 2000*, Boston, MA, Aug. 2000, pp. 255–265.

[12] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *WiSe'02: Proc. of 1st ACM Workshop on Wireless Security*, Atlanta, GA, Sep. 28, 2002, pp. 1–10.

[13] P. Papadimitratos and Z. J. Haas, "Secure link state routing for mobile ad hoc networks," in *IEEE International Symposium on Applications and the Internet-Workshop on Security and Assurance in Ad Hoc Networks*, Orlando, FL, Jan. 2003, p. 379.

[14] T.Haniotakis, S. Tragoudas, and C. Kalapodas, "Security enhancement through multiple path transmission in ad hoc networks," in *2004 IEEE Int. Conf. Communications*, Jun. 2004, vol. 7, pp. 4187–4191.