International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Energy Efficient and Trust Based Node Disjoint Multipath Routing Protocol for WSN

Rucha Agrawal[1], Simran Khiani[2]

[1]PG Student, Computer Engineering, GHRCEM, Pune, India

[2]Assistant Professor, Computer Engineering, GHRCEM, Pune, India

Abstract: ***Wireless Sensor Networks comprises of thousands of sensor nodes that are low power and low cost. WSNs have gained wide applicability recently. Also, the major part of applications are real time and critical like Military, environmental monitoring etc. Thus, WSNs are highly susceptible to vulnerabilities. Hence, security of data is a very important issue. Every layer of the network is subjected to security threat. This paper concentrates on the network layer security. This paper presents a node disjoint multipath routing protocol which is not only energy efficient but also trust based. Energy efficiency is observed by using multipath routing. Also security is imparted by selecting the best path among multipaths based on maximum residual energy and trust among the nodes. Then, public crypto system is applied over the data and it is forwarded through the best path.***

Keywords: Node Disjoint, Multipath Routing, Security, Cryptography, Trust, Encryption, Digital Signature

1. Introduction

A collection of nodes organized in such a way that it forms a cooperative network is called as Wireless Sensor network. These nodes are spatially distributed autonomous sensors. Each sensor node consists of processing capability, may contain multiple types of memory, have a RF transceiver, have a power source, and accommodate various sensors and actuators.

The nodes communicate with each other wirelessly and often self-organize in an ad hoc fashion. Due to its simplicity and wide applicability wireless sensor networks are getting deployed at an accelerated pace. This new technology has wide range of applications. A wireless sensor network is typically a real-time distributed system. Research in Distributed systems generally assumes that the systems are wired and that they have unlimited power. Also, generally, these systems are not real-time. They have user interfaces such as monitors, keyboards and mice. Also, they are location independent. Wireless Sensors network differ in all the above mentioned characteristics. WSN systems are wireless, have very low power, are real-time, use sensors and actuators as interfaces, have dynamically changing sets of resources, aggregate behavior is important and critical location. In spite of several constraints, WSN are used in a variety of applications. The main reason for this is that the sensor nodes consume very less power, they use batteries. Also, the sensor nodes can recover from node failures and also communication failures. Apart from these, nodes are heterogeneous, scalable, can tolerate harsh environmental conditions, are low cost and very easy and simple to use.

The data collected by the sensor nodes are aggregated at the base station or the sink. A base station is a human interface or gateway to another network. It has a larger capacity of processing data or has a larger storage center. Base station can be used to transmit information into the network or extract data from it [16] [17].

Routing the sensed data from the source to the sink node in a resource constrained environment is the major challenge. There are many routing protocols designed and developed specifically for WSNs in which special consideration is given to power management and data dissemination protocols since energy awareness is an essential design issue. Routing protocols are generally application specific. They are broadly classified as single path routing or multipath routing. Single path routing is simple and scalable, but does not efficiently satisfy the requirements of resource constrained WSNs. It is simple because the route between the source node and the destination node can be established in a specific period of time. It is scalable because, even if the network changes from ten nodes to ten thousand nodes, the complexity and the approach to discover the path remains the same. While considering the characteristics of WSNs, single path routing is not as efficient as multipath routing. Multipath routing is an alternative routing technique, which selects multiple paths to deliver data from source to destination. Because of the nature of multipath routing that uses redundant paths, multipath routing can largely address the reliability, security and load balancing issues of single path routing protocols. In Node Disjoint Multipath Routing Protocol, the multiple routes discovered are such that they do not share any common node or link amongst themselves. Thus, if any node fails during transmission of data then only that link or that path is affected. The remaining network remains the same [12][13].

It is very necessary to secure the data at every layer of Wireless Sensor Network. Since routing is one of the most important activities, it is very necessary to provide network layer security.

The main aim of this paper is to design not only energy efficient but also a trust based node disjoint multipath routing protocol for WSN.

2. Existing Multipath Routing Protocols

Hundreds of multipath routing protocols have been designed and developed. While developing these protocols, maximum consideration is given to the energy consumption since it is a

major issue. However, the decision as to which protocol has to be used depends on the application and the network architecture. The routing protocols take into account the metrics like minimum hop, minimum transmission cost, high residual energy to route the data. The following data is from [1][2][3][4][5][6][7][8].
Some of the existing routing multipath protocols along with their advantages and disadvantages are-

Table 1: Comparison of existing routing protocols

Sr. No.	Protocol	Title of paper & Year of Publication	Advantages	Disadvantages
1	AOMDV	On demand multipath distance vector routing in ad hoc networks (2001)	Provides efficient fault-tolerance by faster and efficient recovery from route failures	Message overhead in route discovery and route maintenance is high
2	ENDMSR	Energy aware Node Disjoint Multipath Routing in Moblie Ad Hoc Network (2009)	Cost effective in identifying the multiple node disjoint paths.	Control messages used are higher.
3	SCMRP	SCMRP: Secure Cluster Based multipath routing protocol for WSN (2010)	Provides security in routing the data using technique like pair wise key distribution.	Consume high energy in resource constrained WSNs.
4	SEEM	Secure and Energy Efficient Data Dissemination Protocol for WSN (2010)	Secure and Energy Efficient.	Control overhead is high as number of control packets transferred is greater.
5	REMP	Reliable and Energy Balancing Multi-Path Routing Algorithm for Wireless Sensor Networks (2011)	Reliable and Energy Efficient.	Once the path is constructed, no security mechanisms are used to transfer data.
6	QEMPAR	QEMPAR: QoS and Energy Aware Multi-Path Routing Algorithm for Real-Time Applications in Wireless Sensor Networks (2011)	Energy efficient and provides higher rate of packet delivery	No security mechanisms embedded. Also path is selected based only on the probability of data sending of node.
7	EENDMRP	Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks (2012)	Highly energy efficient and secure since cryptography is used	Path is selected based only on the residual energy of the nodes. No other parameter is considered for path selection
8	SMEAR	Slot Management Based Energy Aware Routing For Wireless Sensor Networks (2013)	Highly energy efficient	While choosing the final path only the energy consumption is considered. No other factor is taken into account.

Due to the highly resource constrained environment of sensor nodes, it is very difficult to embed the security mechanisms used for the traditional networks into the Wireless Sensor Network. Also, some characteristics are unique to WSN which separate it from a typical computer network. Thus, special security mechanisms need to be designed and developed for ensuring that the data from sensor networks is confidential and trusted. Some of the attacks on each layer as mentioned in [9][10][11] are-

A. Attacks on Routing Protocols
Apart from layers of network, security threats also occur on routing protocols. There are several types of routing protocols developed and each protocol is subjected to different types of attacks. Some of the attacks on routing protocols are-

1) *Routing table overflow:* In multipath routing, each node creates its own routing table to forward the data packets to correct destination. In this attack, the adversary advertises false routing information i.e. information about non-existent nodes to the authorized nodes in the networks. Thus, the routing tables of authorized nodes overflow and it prevents the entry of new authorized nodes into the routing table.
2) *Routing table poisoning:* In this attack, the adversary sends non real routing updates to the real nodes so that wrong routing updates are made. This may result into routing loops and congestion in the network.
3) *Packet Replication:* In this attack, the stale or unused packets are replicated by the adversary and sent onto the network. This results into unnecessary bandwidth consumption and also extra usage of other valuable resources of the nodes.
4) *Route Cache Poisoning:* Along with routing table, in certain protocols the nodes also maintain a routing cache to keep the information of the routes discovered in the recent past. The adversary may not only alter the information contained in the routing table but also in the routing cache.
5) *Rushing Attack:* This attack is mainly observed in protocols in which the nodes drop the duplicate packets they receive. Whenever an adversary receives a Route Request packet it immediately forwards the same to all the other nodes so that all the nodes include this adversary in their paths and drop any other RREQ packets that they receive from the honest nodes. Thus, the adversary gets the total access of the network.

Just like any other network, WSN is a layered model and hence threats occur at each and every layer. Also, the category and intensity of threat is different at different layers.

Some of the threats that occur at different layers can be given as-

Table 2: Layer Based Attacks Classification

Sr. No	*Layer*	*Attack*	*Counter measure*
1	Physical Layer	•Jamming •Tampering	Spread-spectrum technique
2	Link Layer	•Exhaustion	Error-correction code
3	Network Layer	•Spoofed routing Information •Selective forwarding •Sinkhole •Sybil •Wormhole •Black hole and Gray hole •Information Disclosure •Resource Depletion •Acknowledgement Spoofing •Hello Flood	Authentication, trust among nodes
4	Transport Layer	•Flooding •Desynchronization	Client Puzzles, Authentication

Thus from the above survey, it can be seen that WSN is subjected to various types of attacks. Of these, the network layer attacks are very common and large in number. Also, the routing takes place at the network layer. This paper proposes a routing protocol in which trust among the nodes is calculated and depending on this value, the best path is selected for propagation of data.

3. Proposed System

A. Problem Statement

To design a node disjoint multipath routing protocol for Wireless Sensor Networks with following factors-

i. Fast and energy efficient route construction in WSN using Fuzzy Astar Algorithm
ii. Calculation of Trust between nodes
iii. Secured Data and Control packet transfer

B. Algorithm

Step 1: Multipath routes from each node are found out and routing table for each node is generated. This is done using the fuzzy astar algorithm as in [18]

It helps in construction of multipaths based on the residual energy in the nodes.

Step 2: Calculate the trust among nodes. For this purpose, first calculate no. of successful packets transferred between every pair of nodes of all the paths in a time period (Δt) denoted by succ. pkt(Δt). Then, calculate no. of unsuccessful packets transferred between every pair of nodes of all the paths in a time period (Δt) denoted by unsucc. pkt(Δt).

Now, T_{ij} , the trust value between two nodes i and j for time Δt is given by[15],

$$T_{ij} = \frac{10 \times succ\ pkt\ (\Delta t)}{succ\ pkt\ (\Delta t) + unsucc\ pkt\ (\Delta t)} \text{ X } \frac{1}{\sqrt{unsucc\ pkt\ (\Delta t)}} \text{-----(1)}$$

The trust value of all the paths is calculated as,

$$T_{pmi} = \sum_{i=1}^{k} T_{i,i+1} \text{----------(2)}$$

The average trust value of each path can be found as,

$$T_{Pmi} = (T_{pmi} / k) \text{--------(3)}$$

Where k=total no. of nodes in a path

Step 3: The best path is then chosen by the attribute weighing method as,

$$P_w = (\alpha \text{ x (Lowest R.E. value)}) + ((\alpha - 1) \text{ x } T_{Pmi}) \text{-----(5)}$$

α=Constant

This path is then chosen for data transmission. To impart additional security, the data packets are subjected to authentication using Digital Signature.

The MD5 hash function H is used to create message digest H(M) at the source node. The source node generates the digital signature, $d_{sign} = (H(M))^d \bmod n$ by encrypting the message digest H(M) with its private key d where, n = p * q, p and q are random prime numbers with $p \neq q$. The source node forwards d_{sign} with data M, (d_{sign}, M) to its neighboring node through the path it takes to reach sink.

A neighboring node on reception of (d_{sign}, M) and the path in the data packet, verifies the digital signature by comparing decrypted value of $d^e_{sign} \bmod n$ with message digest H(M). The $d^e_{sign} \bmod n$ is decrypted using the key (e, n) using sender's public key,

$d^e_{sign} \bmod n = ((H(M))^d \bmod n)^e \bmod n = (H(M))^{ed} \bmod n$

By applying Little Fermat's and Chinese Remainder Theorem to Equation (5), it can be shown that-

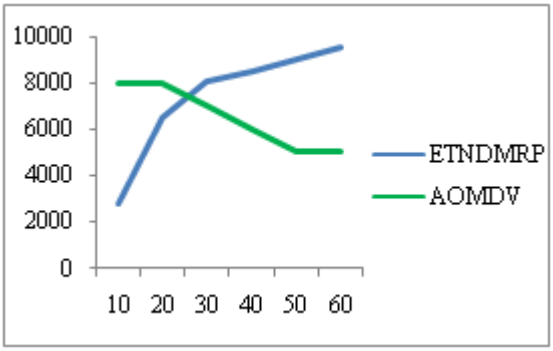
$$d^e_{sign} \bmod n = H(M) \text{ ---------(6)}$$

If the generated H(M) by the receiver and the decrypted H(M) of digital signature dsign is equal, then the receiver accepts the data; otherwise rejects the data and informs the sender that the data is altered through by generating route error packet. This process is repeated in every hop of the node disjoint path between source and destination.

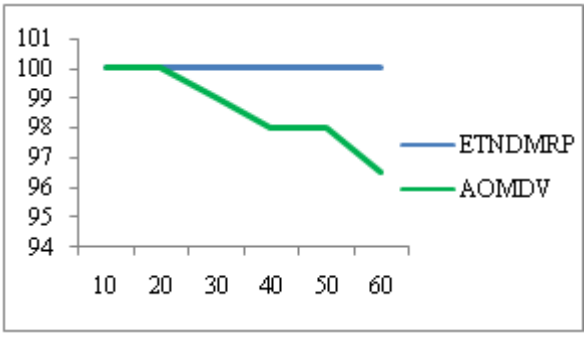
4. Results

The following results are observed when compared with AOMDV-

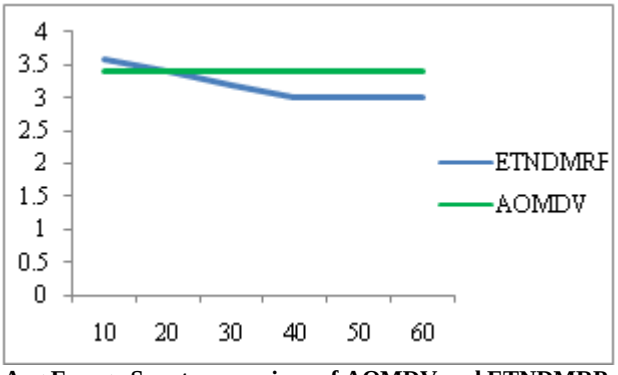
- Packet delivery fraction in AOMDV is reduced to 96.5% for 60 nodes whereas it is 100% for our system.
- Throughput of AOMDV gradually decreases as number of nodes increases whereas it always increases in our system.
- Average Energy spent is slightly less as compared to AOMDV



Throughput comparison of AOMDV and ETNDMRP



PDF comparison of AOMDV and ETNDMRP



Avg Energy Spent comparison of AOMDV and ETNDMRP

5. Conclusion

Since WSNs are used in a wide variety of applications, it is necessary to provide security to it. Also, since major set of attacks take place at network layer and during routing of data, hence providing network layer security is very essential. This paper aims to design and implement a node disjoint multipath routing protocol which is-

- Energy Efficient because while selecting the best path among all the available paths, the path with maximum residual energy is selected
- Trust based because along with residual energy consideration, the path with maximum trust value among the nodes is selected.
- Security of data is observed by using digital signature crypto system.

References

[1] M. Marina and S. Das, "On-demand multipath distance vector routing in ad hoc networks," in *Proc. Int. Conf. Netw. Protocols*, 2001, pp. 14–22.

[2] M. Bheemalingaiah1, M. M. Naidu2, D. Sreenivasa Rao3, G.Varaprasad4, "Energy Aware Node Disjoint Multipath Routing In Mobile Ad Hoc Network", Journal of Theoretical and Applied Information Technology, 2009

[3] S. Kumar and S. Jena, "SCMRP: Secure cluster based multipath routing protocol for wireless sensor networks," in Proc. 6th Int. Conf. Wireless Commun. Sensor Netw., 2010 pp. 1–6.

[4] Neeraj Kumar1, Manoj Kumar1, and R. B. Patel2, "A Secure and Energy Efficient Data Dissemination Protocol for Wireless Sensor Networks", International Journal of Network Security, Vol.15, No.6, PP. 490{500, Nov. 2013

[5] A. Ghaffari, N. Firuz and H. Bannaeian, "REMP: Reliable and Energy Balancing Multi-Path Routing Algorithm for Wireless Sensor Networks", World Applied Sciences Journal 15 (5): 737-744, 2011 ISSN 1818-4952 IDOSI Publications, 2011

[6] S. Heikalabad, H. Rasouli, F. Nematy and N. Rahmani, "QEMPAR: QoS and Energy Aware Multi-Path Routing Algorithm for Real-Time Applications in Wireless Sensor Networks", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 1, January 2011 ISSN (Online): 1694-0814

[7] Shiva Murthy G, Robert John D'Souza, and Golla Varaprasad," Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks", IEEE Sensors Journal, Vol. 12, No. 10, October 2012

[8] M. Shahbaz and Ramesh T. M, " Slot Management Based Energy Aware Routing for WSN", ISSN 2319-2526, Volume-2, Issue-4, 2013

[9] A. Singla and R. Sachdeva , " Review on Security Issues and Attacks in Wireless Sensor Networks", IJARCSSE, ISSN: 2277 128X, Volume 3, Issue 4, April 2013

[10] A. Sastry, S. Sulthana and S. Vagdevi, "Security Threats in Wireless Sensor Networks in Each Layer", Int. J. Advanced Networking and Applications Volume: 04 Issue: 04 Pages:1657-1661 (2013) ISSN : 0975-0290

[11] J. Lotf, S. Hossein, N. Ghazani, "Security and Common Attacks against Network Layer In Wireless Sensor Networks", J. Basic. Appl. Sci. Res., 2(2)1926-1932, 2012

[12] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: A survey," Comput. Netw., vol. 11, no. 6, pp. 6–28, 2004.

[13] Marjan Radi 1, Behnam Dezfouli 1, Kamalrulnizam Abu Bakar 1 and Malrey Lee 2, "Multipath Routing in Wireless Sensor Networks: Survey and Research Challenges", Sensors 2012, 12, 650-685; doi:10.3390/s120100650

[14] S. Rehman, M. Bilal, B. Ahmad, Khawaja Muhammad Yahya, A. Ullah and O. Rehman, "Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN)", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012 ISSN (Online): 1694-0814

[15] X.Li,F. Zhou and J. Du, "LDTS:A Lightweight and Dependable Trust System for Clustered Wireless Sensor

Networks", IEEE Transactions on Information Forensics and Security, Vol 8, No 6, June 2013
[16] Sensor Networks: Evolution, Opportunities, and Challenges
[17] Wireless Sensor Networks: Applications and Challenges of Ubiquitous sensing
[18] I. AlShawi and L. Yan, "Lifetime Enhancement in Wireless Sensor Networks Using Fuzzy Approach and A-Star Algorithm", IEEE Sensors Journal, Vol. 12, No. 10, Oct 2012