ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

Energy Efficient Trust Based Routing and Attack Detection in WSN

Trupti Bomble[1], Prof. M. D. Ingle[2]

P.G. Student, Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India[1]

Asst. Professor, Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India[2]

ABSTRACT: Wireless sensor networks are up-surging as a looming technology by the root of their immeasurable span of utilizations in diversified domains. But WSN have stipulations as a root of the sensors saving proficiency limit, transportation frequency range and assessment proficiency. By virtue of the barred valuables and their disregard atmosphere, they are greatly defenceless to diverse types of attacks. Alive system named ActiveTrust considers Black hole attack and contributes trust dependent routing proposal. The greatest fateful introduction of ActiveTrust is that it obstructs black holes with the effectual procreation of a number of enlightenment paths or routes to instantaneously reveal and appraise nodes trust readings and accordingly boost the information route security. In extant system, the trust readings for node were appraised haphazardly, which is not avaricious in terms of appraising prestige of the node in the network. On the ground in forecasted proposal, some specifications such as error rate, latency, and lingering energy are conceded. On the basis of these specifications trust readings will get estimated by the trust manager node and this will enhance the reliability and adeptness of the data packet shipment in WSN. In order to provide security to the data, hashing algorithm named SHA is used to calculate hash values. Also in inclusion of black hole attack, other types of attacks such as DOS, Eavesdropping, Selective Forwarding, Modification of Message, Grayhole, etc are deliberated in projected proposal. The forecasted proposal will be rewarding to work with both the above mentioned attacks.

KEYWORDS: Attacks, Network lifetime, Trust, Hashing, Wireless Sensor Networks.

I. INTRODUCTION

A wireless sensor network normally includes a giant volume of flat-powered, flat-rate grasping gadgets with barred computation, memory and communication assets. Wireless sensor networks (wsns) are up-surging as a looming technology by the root of their immeasurable span of utilizations in diversified domains in industrial, atmosphere monitoring, military and civilian domains. Remote sensor network encloses a few number of sensor nodes which are dispersed in an ambition of diagnosing environment inside of its neighbourhood, congregate the information and processes it. Mobile nodes are composed of basic processor, application peculiar sensors, wireless transceiver and small battery. Due to economic considerations, the sensor nodes are usually straightforward and low cost. Sensor nodes have finite reckoning power, battery, less saving capacity. Since of every one of these confinements, there is an obligation of diminishing so as to save such assets and the amount of data transmission. This can be achievable by correctly electing the route from source to destination in order to transport the data packets in power profitable aspect as shown in figure 1.

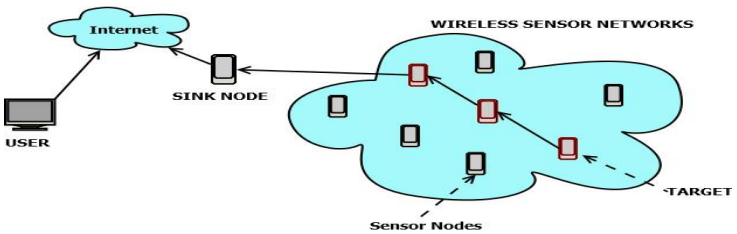

Figure 1. Wireless sensor network

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

They are usually disregarded, however, and are therefore prone to endure from diverse types of novel attacks. Also sensor nodes are bounded in terms of power. So there is a necessity of such a scheme which will securely transport the data packets from sender to receiver via secure precise path. Prior techniques such as active trust, h-spread, MDA, etc considers only black hole type of attack. In networking, black holes are nothing but the points in the network where arriving or extroverted traffic is calmly abandoned, without notifying the source that the data did not received at its destined receiver. Hence it is imperative to take into account other attacks such as denial of service attack, spoofing, sinkhole, sybil, eaves-dropping, etc. A denial-of-service attack (dos attack) is a cyber-attack where the criminal explore to make a network resource or assets nonexistent to its authorised users by transiently or endlessly disorganizing services of a server linked to the internet. Denial of service is commonly adapted by flooding the intended node or resource with excessive requests in a try to overburden systems and avert some or all authorised requests from being accomplished. The controversy of securely transmitting the data packets in WSN with superior energy adaptability in the existence of denial of service and other type of attack should be consider.

II. RELATED WORK

In paper [1], authors have proposed active detection based security and trust routing technique for wireless sensor network called as ActiveTrust. In this, numbers of detection routes are actively created to immediately detect and calculate nodes trust values in order to enhance the data packet route security.

H. Sun, C. Chen, Y. Hsiao [2], In this, MDT strategy is used which isolates the network into two dataflow topologies. Alike if one topology has a mischievous sensor node, the BS can still receive data packets via other topology.

W. Lou, Y. Kwon, [3] H-SPREAD integrates the path formation process and hybrid message transportation scheme. It holds the benefits of a threshold secret sharing and route diversification of multipath data promoting to boost path flexibility against node breakdown or compromise routes. Data packets can be protectively forwarded towards the sink node even when a short number of sensor nodes or routes have are attacked during the data transportation process.

A.Liu, M. Dong, K. Ota, et al [4] A Per-Hop Acknowledgement(PHACK)-based technique is introduced for every packet transposition to find selective forwarding attacks. Here, the BS and every sensor node along the prolonging path produce an (ACK) acknowledgement / feedback message for every obtained packet to certify the ordinary packet transmission.

T. Shu, M. Krunz, S. Liu [5], have introduced a randomized multi-path routing procedure. In this algorithm estimates various paths in a arbitrary manner every time an information packet wish to be transmit, such that the set of paths taken by multiple shares of distinct packets keep altering over time. As an outcome, a more number of routes can be possibly produces for each source and target.

P. Zhou, S. Jiang, A. Irissappane, et al. [6], have exposed the ineffective utilization of watchdog mechanism in currently available trust systems, and by that proposed a series of escalation methods to reduce the energy expenditure of watchdog usage, while maintaining the system's security in a satisfactory level.

In this paper [7], authors have proposed a new trusted path which considers communication reliability and route length for a reliable and feasible date packet delivery in a MANET. Authors have proposed the term called attribute similarity in detecting possibly friendly sensor nodes among strangers; so security is inherently added into the routing protocol where nodes estimates trust levels of others on the basis of a set of attributes.

In this paper [8], Authors have proposed a RBR technique to focus on the issue of sink-position secrecy. Under the RBR technique the routing rings move in random arrangements which can trouble attackers even if the sink position is static and this extremely enhances the sink-position secrecy.

III. EXISTING SYSTEM

The extant system titled ActiveTrust is power adequate, reliable and secured routing technique. It contributes effective discovery based security and trust routing in WSN. But the advancement in ActiveTrust technique is the estimation of trust values for sensor nodes. Trust value estimation can be more profitable. Appropriate estimation of trust values for nodes can enhance the proficiency of disclosing secure path.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

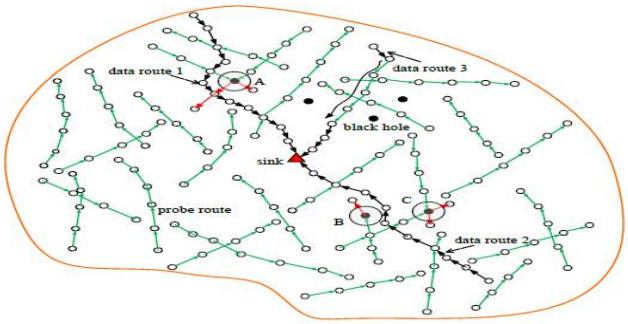

Figure 2. Existing System Architecture

Also the extant system considers only Black hole attack. We can look after other types of attacks in ActiveTrust technique. Figure 2 shows the Interpretation of the ActiveTrust scheme.

IV. PROPOSED SYSTEM

As shown in fig. 3, system looks at the network of number of disposed sensor nodes. One source and destination node is elected among them. Here the destination node is Base station. For transporting or routing data packets from source node to destination node (BS), numbers of multiple paths are estimated using path calculation/ estimation model. While electing the shortest and power profitable path among available paths, some specifications are taken into account such as nodes trust values, error rates, latency, and leftover energy of each node. On the basis of these specifications Trust evaluation model is designed. The node called Trust manager node, calculates trust and reputation of each node. At last the path which is energy profitable, reliable and secure is elected to transport the data packets from source node to destination node. Considering security aspect of data, hashing is performed on the data at source side. On receiving side hash value is recalculated to check for data integrity. Fig. symbolizes the system architecture.

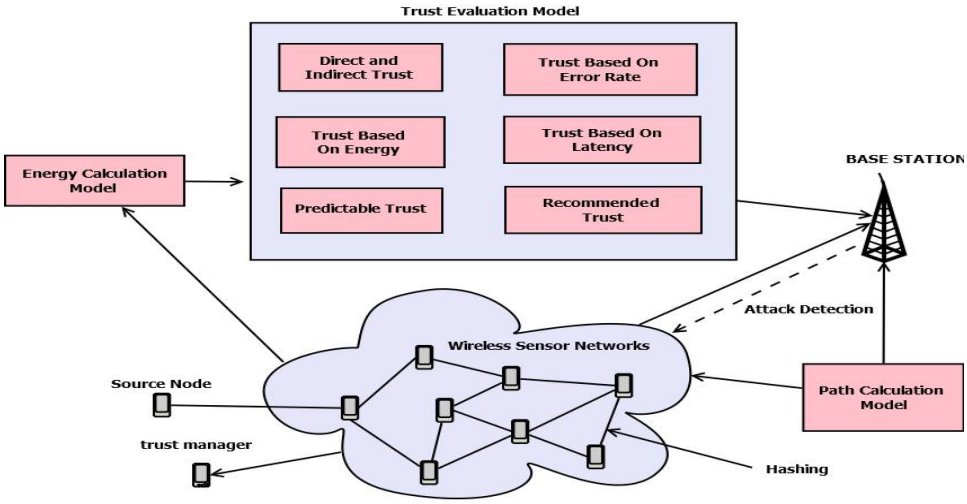

Figure 3. Proposed System Architecture

The System is split into number of stages which are interpreted as follows:

- Network deployment- In this the input i.e. number of sensor nodes to be deploy is taken from user and the network of sensors is created. Among the sensors in network, one node is the target i.e. Base station and another is selected as a source node.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

- Trust Evaluation Model- In trust evaluation model, trust manager node collects information of all nodes and calculates trust and reputation of each n every node on the path. Trust value for each node will be estimated on the basis of: direct and indirect trust, trust based on energy, trust based on error rate, trust based on latency. Trust value of specific node will be incremented by one if the data packet is successfully transported through it otherwise trust value is decremented by one. The node or specific zone or route which is having greatest trust values is considered as more secure and reputed for sending the data.
- Route discovering model- In this model, the number of routes will be discovered from source to destination. And depending on some specifications such as the minimum number of in-between hops, minimum utilization of power and maximum remaining energy of nodes, maximum trust count of the node, etc, the proper route will be selected for sending the data.
- Hashing and sending data- In this, the hashing function is used to calculate the hash value of the data to be transmitted. Hashed data is then sent to the destination through trusted route. At receiving side, hash value is recalculated in order to provide security to data.
- Discovering and prohibiting attacks- In this model, discovery and avoidance of Black hole attack as well as other attacks will be detected in order to find altered and dropped data packet.

V. MATHEMATICAL MODEL

Mathematical Model for Proposed Work:
For Energy Calculation :
Etx (k; d) = Eelec * K+ 2amp * k * dn …… {Energy Required for transmission}
ERx(k) = Eelec * k ……. {Energy Require for Receiving Packets}
d: Distance for neighbouring sensor node.
2amp: Energy required for the transmitter amplifier.
Eelec: Energy consumed for driving the transmitter or receiver circuitry.
k = bits per message.
Above formula is used to calculate the energy required to transfer the data. So,

Nodes updated Energy=Available Energy – Energy Consumed;
Error Rate = Number of Packets Send - Number of Packets Received;
Latency (in ms) = Packet Received Time - Packet Send Time;

Trust Calculation :
Available Trust (Tava) = Trust value of that node.
Average Trust (Tcal) = Calculated based On (Error Rate, previous Successful Transaction, latency);
Direct trust (tdx): Trust assigned directly after transaction.
Recommended Trust (trx) = recommended trust from neighbours.
Indirect Trust (tix) = trx + Tcal.
Forgetting factor (β) = 0< β<1
Nodes Present Trust value = Tava + tdx + tix + β; // (If Successful Transaction) where, $\beta < 0.5$
Nodes Present Trust value = Tava - tdx - tix - β; // (If Unsuccessful Transaction) where, $\beta > 0.75$

Hashing
A hash function: H: k * D -> R
Where,
D is the domain of H and R is the range of H
If K € k is a particular key then Hk : D -> R is defined for all
M € D by Hk(M) = H(K,M)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

VI. ALGORITHM

Input: N (no. of nodes)
Output: Secured data at Destination node.
1) Start
2) Deploy sensor nodes network.
3) Register all nodes to Trust Manager and authenticate them
5) Select Source Node and Destination node.
6) Calculate hash at the source.
7) Calculate all paths from source to destination.
8) Calculate the trust of all nodes on the path.
9) Select the shortest and trusted path for routing data.
10) Send data through selected path.
11) Recalculate hash at destination node.
12) Authenticate data.
13) Calculate the size of data received at destination node.
14) Increment or decrement the nodes trust value on the basis of size of data at the time of sending and receiving.
15) Detection of BLA and other type of attacks.
16) Repeat from step 5
17) Stop

VII. EXPERIMENTAL SETUP

The system developed in Netbeans (version 8.1) tool using Java framework (version jdk 8) on Windows platform. The network is generated using Jung tool in which contain sensor nodes. The system doesn't need any specific hardware to run, any standard machine is capable of running the application.

VIII. IMPLEMENTATION

As shown in figure 4, Data is send over the selected path. Path is selected on the basis of remaining energy and calculated trust. Initial trust and energy is assigned to each node by the base station.

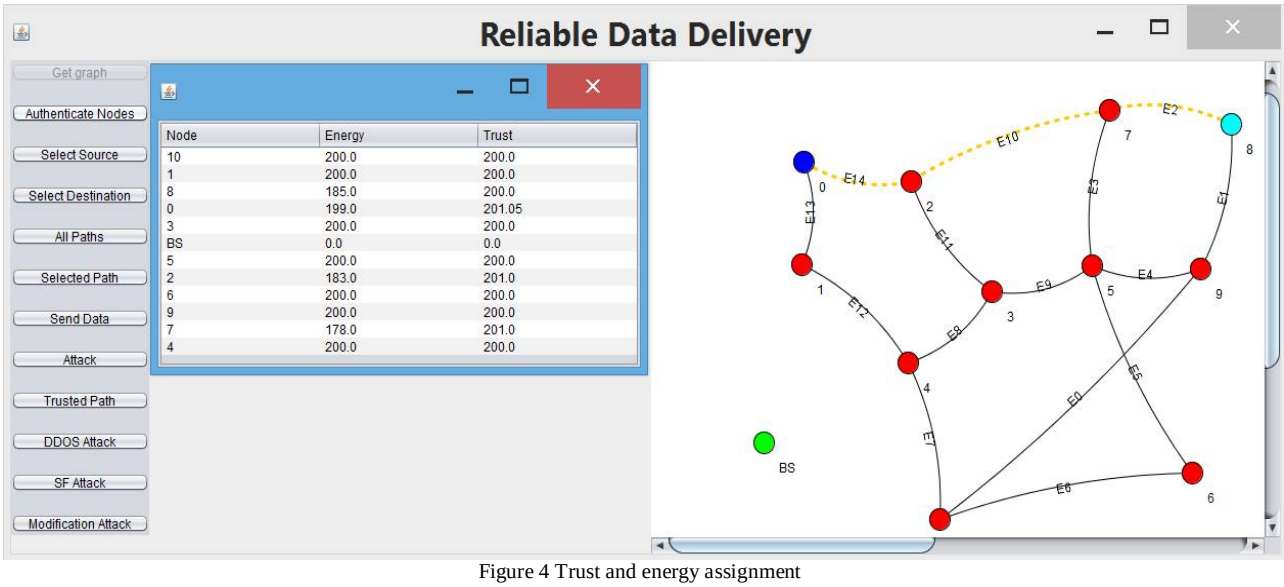

Figure 4 Trust and energy assignment

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

As shown in figure 5, DOS attack is performed on the node from path. The system identifies and blocks the unauthorised node who tries to perform DOS attack on path.

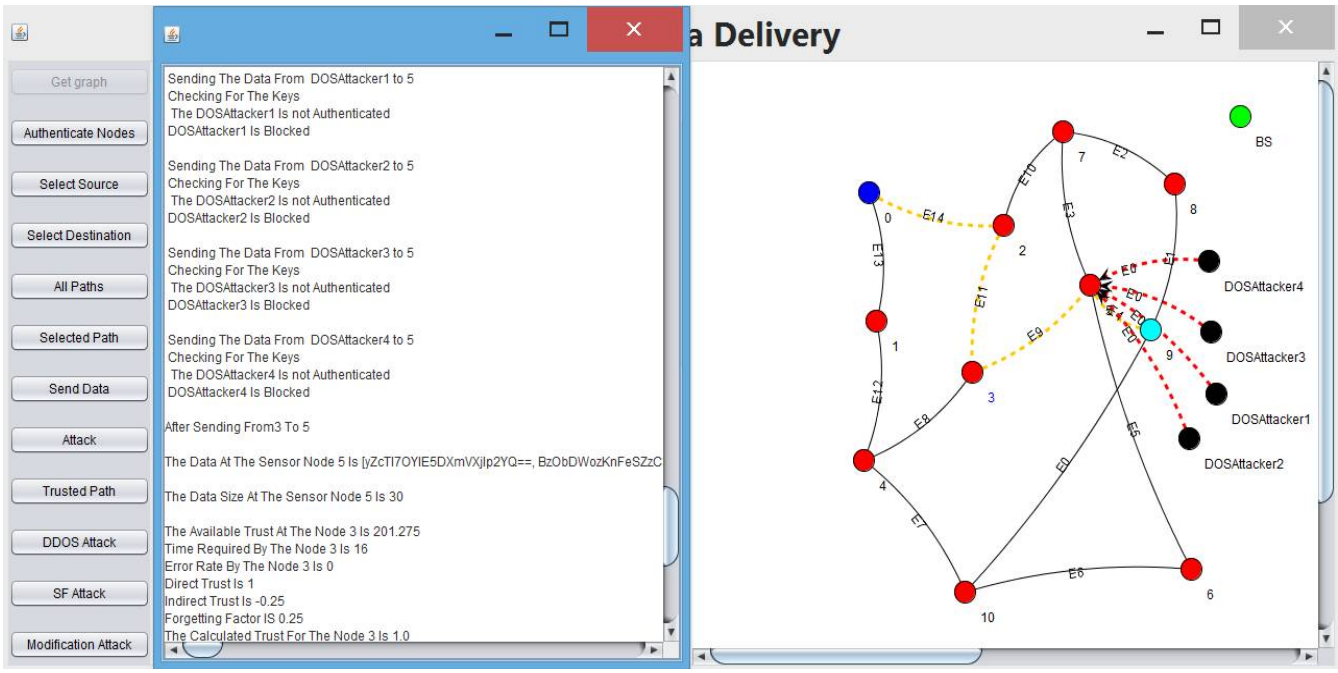

Figure 5 DOS attack detection and prevention

As shown in figure 6, data modification attack is detected and alert message on detection is displayed.

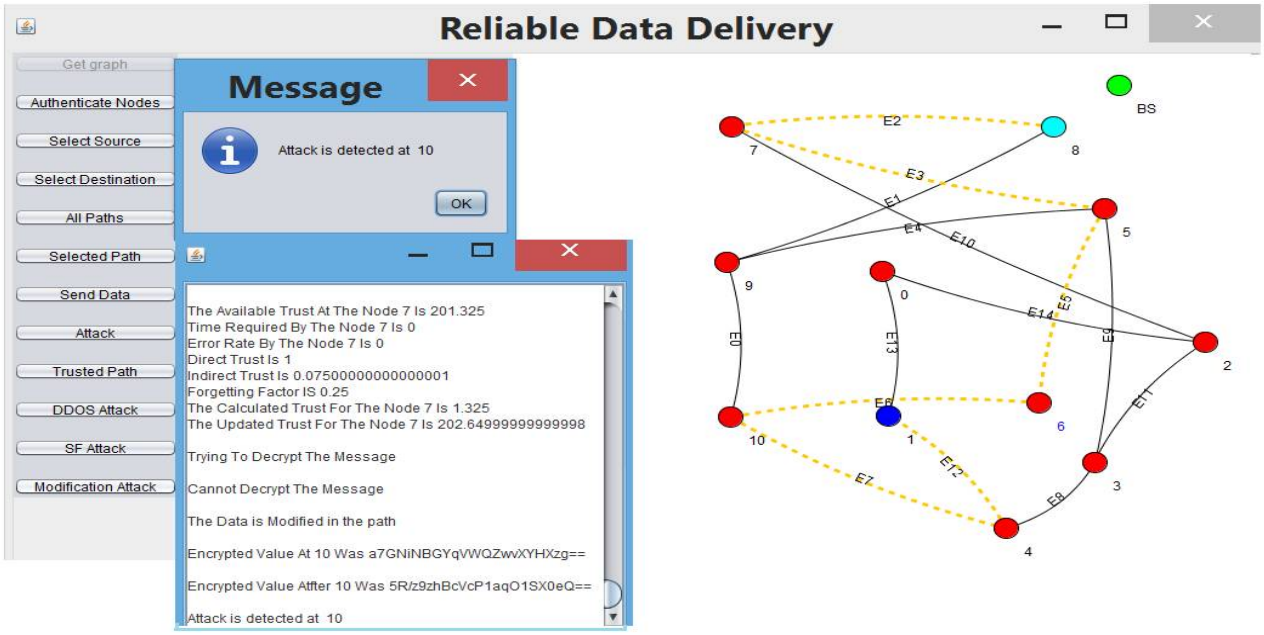

Figure 6: Modification of Message Attack detection and Prevention

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

IX. SYSTEM ANALYSIS

A. Energy Graph

Figure 7 shows the comparison graph for energy consumption ratio of existing and expected system. We expect that the energy consumed by the propose system will be less as compared to existing system.
Following table 1 shows the comparison of existing and proposed system in terms of energy.

Table 1. Energy comparison between existing and expected system

Work Task	Existing System	Expected System
Energy	550	400

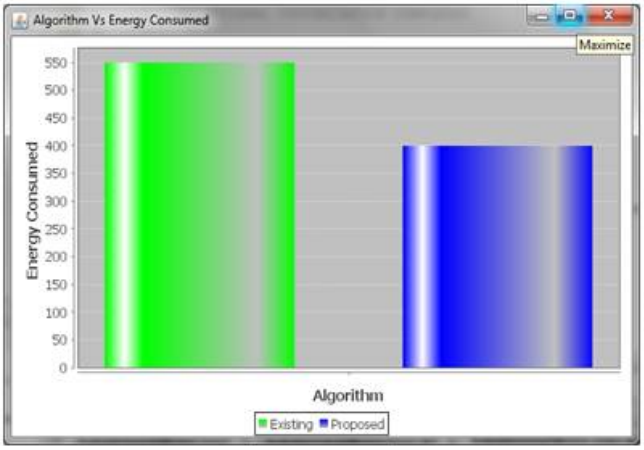

Figure 7. Energy Comparison between Existing and Expected system

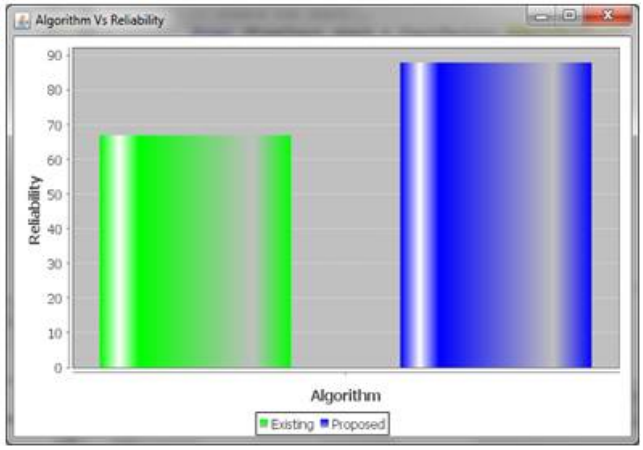

Figure 8. Reliability between Existing and Expected System

B. Reliability Graph

Figure 8 shows the comparison graph for reliability of existing and expected system. Existing system is less reliable as compared to expected system.
Following table 2 shows the comparison of existing and proposed system in terms of reliability.

Table 2. Reliability comparison between existing and expected system

Work Task	Existing System	Expected System
Reliability	69	89

B. Time Graph

Figure 9 shows the comparison graph for time of existing and expected system. Existing system is more time consumable as compared to expected system.
Following table 3 shows the comparison of existing and proposed system in terms of time.

Table 3. Time comparison between existing and expected system

Work Task	Existing System	Expected System
Time	700	500

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

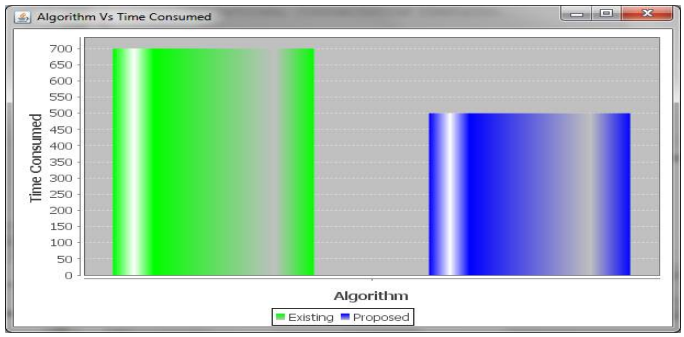

Fig.9 Time Comparison Graph between existing and proposed system

X. CONCLUSION

After doing the survey of extant systems for reliable and power profitable shipment of data in WSN, we found the Active trust technique as more profitable. Therefore, contributes an enhancement over the extant active trust technique. Nodes trust values are estimated depending on number of favourable transportation of right data via that node. This makes extant system more prosperous and exact in terms of disclosing prestige of node in peculiar zone of network. Our system will be more power profitable, reliable and secure as we are transporting the data via the shortest route which is chosen on the basis of some specifications such as nodes trust values, latency, error rate, etc. Also we taken the look on the fact that distinct types of attacks such as denial of service attack, black hole attack can happen on WSN and accordingly we will provide the solution for disposing such attacks. In future work, we will interrogate the approach on more number of attacks in WSN.

XI. ACKNOWLEDGEMENTS

It is pleasure for me to thank lot of people who have support me in completing to this paper in different ways. Starting with, I would like to thank my Guide, Prof. M. D. Ingle for his support during the entire work. His support for helping me to get helpful content in the topic. I am thankful to HOD, Principal, teachers and collage to providing us the facilities in the department and their guidance.

REFERENCES

[1] Yuxin Liu, Mianxiong Dong, Member, IEEE, Kaoru Ota, Member, IEEE, Anfeng Liu, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, 1556-6013 (c) 2016
[2] H.Sun, C. Chen, Y. Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor networks," in Proc. Of IEEE TENCON 2007, pp. 1-4, 2007.
[3] W. Lou,Y.Kwon, "H-Spread: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks," IEEE Transaction on vehicular technology, vol. 55, no. 4, pp. 1320-1330, 2006.
[4] A.Liu, M.Dong, K.Ota, et al. "PHACK:An Efficient Scheme for Selective Forwarding Attack Detecting in WSNs," Sensors, vol. 15, no. 12, pp. 30942-30963, 2015.
[5] T. Shu, M. Krunz,S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 941-954, 2010.
[6] P. Zhou, S. Jiang, A. Irissappane, et al. "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 613-625, 2015.
[7] J.Wang, Y. H. Liu, Y. Jiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length," Journal of Network and Computer Applications, vol. 34, no. 4,pp. 1138-1149, 2011.
[8] J. Long, A. Liu, M. Dong, et al. "An energy-efficient and sink-location privacy enhanced scheme for WSNs through ring based routing," Journal of Parallel and Distributed Computing, vol. 81, pp. 47-65, 2015.
[9] T. P. Nghiem, T. H. Cho, "A multi-path interleaved hop-by-hop en-route filtering scheme in wireless sensor networks," Computer Communications, vol. 33, no. 10, pp. 1202-1209, 2010.
[10] I. Aad,P. J. Hubaux and W. E. Knightly, "Impact of Denial-of-Service Attacks on Ad-Hoc Networks," IEEE-ACM Transactions on Networking, vol. 16, no. 4, pp. 791-802, 2008.