International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 6 (2015) pp. 14727-14738

http://www.ripublication.com

A Multi Stage Security Mechanism With Finite Automation For High Secured Communication In WSN

N.Vadivelan[1*], S.Anbu[2]

[1]Research Scholar, Department of Computer Science and Engineering, St.Peter's University, Avadi, Chennai, India, email: vadivelanresearch@gmail.com*

[2]Professor, Department of Computer Science and Engineering, St.Peter's College of Engineering and Technology, Avadi, Chennai, India, email: anbuss16@gmail.com

Abstract

Security in Wireless sensor systems is one of the real issues; hence a lot of research is done on numerous routing attacks on WSN. Due to the very nature of wireless sensor network, a malicious node creates itself automatically in WSN. Therefore a **MSSM** – [Multi Stage Security Mechanism] is proposed to provide a stage by stage security for every node presented in the network. Init-Stage, Service-Stage and Destroy-Stage are the three stages considered the life-cycle of a node in WSN. Registration and Recoding in Init-Stage, Verification and Validation in Service-Stage and Candidate-Closing in Destroy-Stage are the stages wherein the security is applied. Each stage of MSSM is activated and deactivated using Finite Automation. The MSSM algorithm is actualized in Network Simulator and the performance metrics such as throughput, Energy, malicious node detection rate and Packet delivery ratio are verified.

Keyword: Wireless Sensor Network, Security, Secured Communication, Finite Automation.

Introduction

Improvement of sensor frameworks as one of the transcendent advancement inclines in the approaching decades has posed diverse troubles to researchers. The advancement of remote sensor systems was necessitated by military provisions, for example, front line observation. Today such systems are utilized within numerous modern and buyer provisions, for example, mechanical methodology check and control, machine wellbeing observance, environment and living space observance, health awareness provisions, home computerization, and activity control. Guiding Protocols for remote sensor networks should address troubles like lifetime support, power, inadequacy tolerance and course of plan to all the nodes.

An infrastructure less network having sensor nodes with wireless communication medium are defined as the WSN. Communication between two nodes is achieved through multi-hop wireless connection. Entire nodes in the network can also act as a router, which can forward data to other nodes. Nodes are independent can move from one place to another place in any direction. Because of nodes mobility there will be a continuous link breakage is happening in the network. WSN is very popular due to its emerging application nowadays. Very important designing in WSN is QoS based. By configuring and making changes in the network features, it is easy to improve the QoS factors in a network. The motto of this paper is to construct and implement a technique for doing well on QoS factors in terms of Security and Energy consumption. To achieve the aim the contribution of the MSSM is focused on providing stage wise security in the network.

Background Study

Since WSN is dynamic and is drastically growing, it is be deployed in emerging situations, mostly interconnecting and communicating with various other networks. Hence a malicious node created automatically or with the help of other malicious nodes. The main problem to be considered is multi-hop communication in WSN. A malicious node can affect the performance of the network. In certain kind of applications like medical and military, security is the most important in WSN. In, one of the papers the author proposed the instrument for securing the QoS course and to expand the likelihood of achievement in discovering QoS in both possible ways. Giving both security and QoS as directed in MANET is a significant test for this innovation [2]. Yih-Chun Hu et al. talked about and created SQoS, a protected type of QoS-Guided Route Discovery for on-interest specially appointed system directing. SQoS depends completely on symmetric cryptography [3]. CRESQ is also one of the routing protocols introduced for improving the QoS in terms of security and energy efficiency [4].

In [5], the behavior and the necessity of the QoS factors are discussed. In [6], the importance, related issues and significant point of MANET are discussed briefly. Security, multicasting with QoS factors are examined and reported in [7]. Location based power aware routing protocol is described in [8]. By configuring MAC and adjusting bandwidth information [9] the energy is saved and is given in [10]. IEEE 802.11standards can function with any one of the two modes as (a) continuous active mode and (b) power saving mode [11, 12]. By the use of sleep state, the node's power can be saved [13].

The idle state of a node can also help to save the node energy [14] like sleep state. In [15], node wakes-up-scheduling method is used for reducing the power consumption. Cell2Notify mechanism was the energy management architecture in [16] to improve the power consumption effectively in IEEE-802.11 standard networks. Presently, WSN needs a best solution for secured communication [17, 18]. Proposed work in this paper is trying to find a single solution for both issues as security and energy consumption.

Existing System

In the existing system, it was focused on the attack known as sinkhole attack which spoils the complete communication and causes data loss between a pair of nodes the source node and a destination node. In order to provide a complete solution to detect and avoid sinkhole attack a Leader Based Intrusion Detection System (LBIDS) is proposed [1].

Proposed Approach

MSSM Approach

This paper proposes a Multi Stage Security Mechanism which provides Security for Node and its Data. The following Diagram depicts the functionality of Multi Stage Security Mechanism in Fig.1.

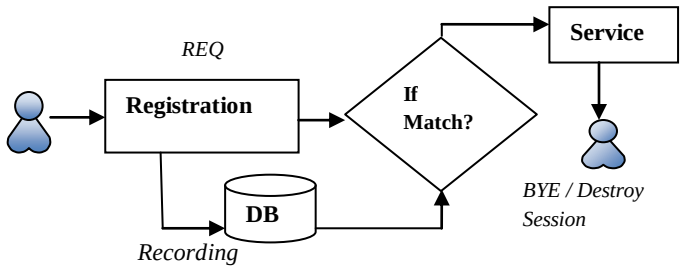

Figure 1: MSSM [Multi-Stage Security Mechanism]

The overall security provision applied in WSN is shown in Fig.1 and the detailed description is given below. A network G is developed with N number of nodes. Where, N = { $N_1, N_2, \dots, N_N$} and each node N_i is placed randomly among a 1500 x 1500 sized region of WSN. Let's assume there are three stages to be considered as the life-cycle of a node, when a node is initialized for network communication the stage is 0 [$\delta = 0$]. When the node transmits the data packets its state is 1 [$\delta = 1$] and when the node completes transmission its state is -1 [$\delta = -1$].

$$Life - Cycle = Init - Stage + Service - Stage + Destroy - Stage$$

To make sure that the node is trust-able node and belongs to the same network, the state of the node is verified for transmitting the data packets. If a node is born in the network it should be initialized in the Init-stage.

SSM: Init-Stage

Network *G* functions under a Base station *B* and *B* has its own administrator *A*, which activates and de-activates the state and stages of a node. $\forall i, N_i$ is assigned by a keyL_{xy} N_{ID} $Count_{NID}$ T and added into N_{TABLE} as a record, where each record has four fields as Count, Node-ID, Time-of-Initialization and Location of the Node-born.The key assignment is called at initialization of nodes in the network and the details of the node are recorded in the database [N_{TABLE}] and its state is set 0 [δ=0].

Only an initialized node can go for further service stage the others are either unknown to the network or considered as malicious.

MSSM: Service-Stage

When a node $\boldsymbol{N_i}$ sends a data packet to node $\boldsymbol{N_j}$ both node $\boldsymbol{i}$ and $\boldsymbol{j}$ should submit their ID, location and their key to $\boldsymbol{A}$. $\boldsymbol{A}$ Verifies their submitted information with the record information in the $[\boldsymbol{N_{TABLE}}]$ and sets their state as $[\boldsymbol{\delta = 1}]$ and check their available state as 0 or not. [If their state is already 1,it means the node is busy]. $\boldsymbol{A}$ confirms, that both nodes $\boldsymbol{i}$ and $\boldsymbol{j}$ are trust-able and their state is ready for data transmission. State$\boldsymbol{\delta = 1}$ indicates that the node is already in the service state. While transmitting data packets the data is encrypted using the RSA algorithm with the node-ID and in destination node, from the packet format the source node-ID is taken for data decryption.

MSSM: Destroy-Stage

After node $\boldsymbol{i}$ receives a confirmation from node $\boldsymbol{j}$ that $\boldsymbol{j}$ received the data packet successfully both node states are set to -1, means that the nodes are ready for the next life-cycle. In this paper, MSSM verifies the node trust-ability and busyness in the various stages then decides and permits the node to serve in the network. MSSM follows AODV protocol with a route - repair mechanism to avoid data loss and increase the success data transmission. The MSSM algorithm is programmed in TCL language in NS2 and the performance is evaluated.

Automata Theory

One of the important tools which can be used to represent the data is $RegEx$ derived from FA-[19]. The life cycle of the MSSM follows the transition state of the FA. Means, the next state of the input character is determined by the previous state and the present input character. The FA is called as DFA or NFA due to the resulting state is unique or not.

$\boldsymbol{N} = \{\boldsymbol{N1}, \boldsymbol{N2}, \boldsymbol{N3} \ldots . \boldsymbol{Nn}\}$,

are the nodes deployed in the network and

$$\boldsymbol{I} = \boldsymbol{keyL_{xy}}\mathbf{N_{ID}}\mathbf{Count_{NID}}\mathbf{T}$$

is valid input $\boldsymbol{I}$ included in to the regular expression R else no match is returned.

$$\boldsymbol{R1}\colon [\boldsymbol{abcd}]\ \boldsymbol{op} : \boldsymbol{R1}\colon \boldsymbol{a} \rightarrow \boldsymbol{b} \rightarrow \boldsymbol{c} \rightarrow \boldsymbol{d} \rightarrow \boldsymbol{op} : \boldsymbol{R1} : \boldsymbol{abcd} \rightarrow \boldsymbol{c} \leftrightarrow \boldsymbol{d} \rightarrow \boldsymbol{op}$$

$$\boldsymbol{R2}\colon [\boldsymbol{acd}]\ \boldsymbol{op} : \boldsymbol{R2}\colon \boldsymbol{a} \rightarrow \boldsymbol{c} \rightarrow \boldsymbol{d} \rightarrow \boldsymbol{op} : \boldsymbol{R2} : \boldsymbol{acd} \rightarrow \boldsymbol{c} \leftrightarrow \boldsymbol{d} \rightarrow \boldsymbol{op}$$

$$\boldsymbol{R3}\colon [\boldsymbol{ac}]\boldsymbol{op} : \boldsymbol{R3}\colon \boldsymbol{a} \rightarrow \boldsymbol{c} \rightarrow \boldsymbol{op} : \boldsymbol{R3}\colon \boldsymbol{ac} \rightarrow \boldsymbol{c} \leftrightarrow \boldsymbol{d} \rightarrow \boldsymbol{op}$$

$\boldsymbol{abcd}$ represents the input values key, location, node – id and node count with time and the $\boldsymbol{op}$ denotes the state $\boldsymbol{\delta}$.

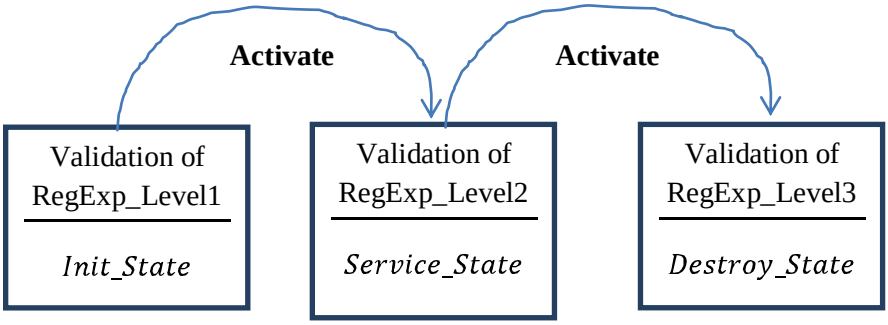

Fig.2: Stage Activation through Automation Theory

The four fields are also called as parameters and they are used to verify and validate the user. The parameters are assigned by the characters as:

$a \rightarrow Key;\ b \rightarrow Node\ Location;\ c \rightarrow Node\ id;$

$d \rightarrow Node - Count\ with\ time$

The characters are combined to form string like ***"abcd"***, ***"abc"***, ***"ac"***, ***"bc"*** and so on. The string patterns are created by verifying the parameters and validated. If the strings are valid then it activate the next state $[\boldsymbol{\delta = 1}]$, else, it de-activate the present state and process is terminated. The $RegExp$ sets are prepared in the $init\ stage$. Before entering into the second stage i.e, $service\ stage$, the $RegExp$ is analyzed by character wise and the combination of character wise. The $RegExp$ is generated for all the nodes in the network and distributed. MSSM verifies the timing of $RegExp$ validation due to the behavior is verified within a time interval. The length of the string may vary to due node mobility. In this paper, there are three things to be analyzed for the three stages, such as maintaining a pointer to the next state and status of the current state and finally verifying the timing values.

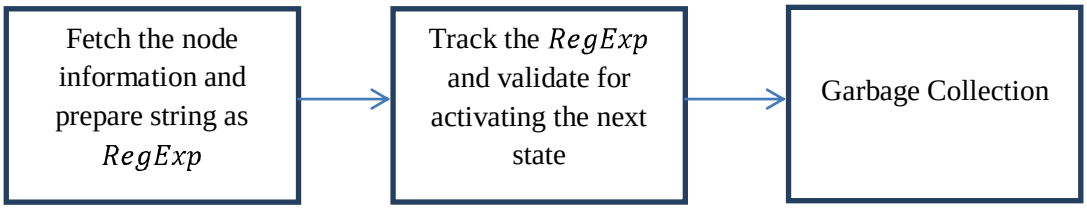

Figure 3: FA for MSSM

Once the preparation and comparison stages are over, finally the $RegExp$ values are assigned to "0" or "NULL" , means applying the garbage collection. By applying this automat theory the entire functionality of MSSM becomes automatic and time effective and cost effective. The following algorithm and Figure-2, Figure-3, Figure-4 and Figure-5 show and prove the performance of MSSM.

$MSSM\_Algorithm( )$

{

1.$Let\ G\ = \{N_1, N_2, \dots, N_N\} \forall\ i \in 1\ to\ N$

2.$For\ I\ =\ 1\ to\ N$

3.Key(N_i) = $concat(L_{xy}, N_{ID,} Count_{NID,} T)$

4.End

5.$For\ I\ =\ 1\ to\ N$

6.If (Key(N_i) == rec(N_{TABLE}])) $then$

7.State(N_i, δ) = 0

8.$Else$

9.Suspect(N_i)

10. End

11. End

12. if (Key(N_i) == rec(N_{TABLE}]) && Key(N_j) == rec(N_{TABLE}])) $then$

13. State($N_{i,j}, \delta$) = 1

14. data(N_i) $\rightarrow data(N_j)$

15. State($N_{i,j}, \delta$) = -1

16. End

}

Simulation Settings

$MSSM\_algorithm$ is programmed using NS2-TCL language. The necessary parameters are assigned with appropriate values to configure the available AODV protocol in Network simulator. To evaluate the performance of the MSSM approach the throughput, Packet delivery ratio, delay, routing overhead and energy are verified and shown in the following figures. And it is evaluated by changing the number of nodes as 10, 20, and 30 to 100.

Table 1: Parameter Settings in Network Simulator 2.34

Parameters	**Value Assigned**
Channel	Wireless Channel
Area defined	1500 x 1500
Number of Nodes	10 to 500
Radio Model	Two Ray Propagation Model
Energy Model	Wireless_Phy- Energy Model
Routing Protocol	HSEERP
MAC	S-MAC
Simulation Time	50 ms
Frequency	2.4 GHz
Bandwidth	Custom
Traffic Type	CBR/VBR/ custom

Throughput*:* The total number of data packets transmitted and received successfully within a stipulated time period.

Packet Delivery Ratio*:* The percentage of received data packets in the destination.

Energy: Remaining Energy of each node is summed after detecting the consumed energy.

Performance Evaluation*:* The number of attacker node detected in the network for various numbers of nodes is compared and the performance of the MSSM is evaluated. For all the QOS metrics the comparison among MSSM and LBIDS is given in the following Fig.2 and Table-1.The energy assigning and computation is given in the following mathematical representations. To compute the energy level of the nodes and network, the two-Ray ground propagation model is used and it uses the distance for communication. For various states like receiving a data packet, transmitting a data packet, idle, listening and sleep, wakeup different amount of energy is reduced from the initial energy of the node. The energy states are updated in each round of the data gathering and data aggregation by the CH in each cluster. The initial energy is initialized as 100 joules. For each state some amount of energy is predefined and assigned.

$$\boldsymbol{Initial\ Energy\ =\ 100\ joules}$$
$$\boldsymbol{Transmitting\ Energy\ =\ 0.26\ joules}$$
$$\boldsymbol{Receiving\ Energy\ =\ 0.08\ Joules}$$
$$\boldsymbol{Idle\ Energy\ =\ 0.01\ Joules}$$
$$\boldsymbol{Sleep\ Energy\ =\ 0.005\ Joules}$$
$$\boldsymbol{Wakeup\ Energy\ =\ 0.005\ Joules}$$

In each round the initial energy is updated using the following formula like

$$\boldsymbol{Remaining\_Energy = Initial\_Energy - [Transmitting\ Energy + Receiving\ Energy + Sleep\ Energy + Wakeup\ Energy + Idle\ Energy + Listening\ Energy]}$$

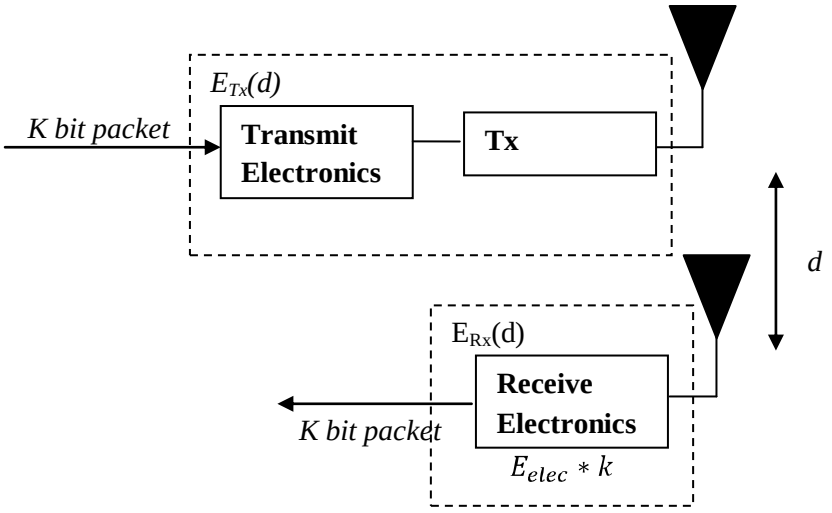

Figure 4: Energy Computation

Where,

$$E_{Tx}(k,d) = E_{Tx} - elec^{(k)} + E_{Tx} - amp(k,d)$$
$$E_{Tx}(k,d) = E_{elec} * k + E_{amp} * k * d^2$$
$$E_{Rx}(k) = E_{Rx} - elec^{(k)}$$
$$E_{Rx}(k) = E_{elec} * k$$
$$E_{Tx} \rightarrow Tramission\ Energy$$
$$E_{Rx} \rightarrow Recieving\ Energy$$
$$k \rightarrow Number\ of\ Bits\ in\ a\ packet$$
$$d \rightarrow Distnace\ among\ the\ nodes$$

If a node loses it energy completely then the node energy is reinitialized in Network Reconstruction phase after a number of rounds or after a stipulated time.

Table 2: MSSM vs. LBIDS Comparison in Terms of Number Malicious Node Detection

No. of Nodes	10	20	30	40	50	60	70	80	90	100
LBIDS	1	2	3	4	5	6	7	8	9	10
MSSM	0	0	0	1	1	1	1	2	2	2

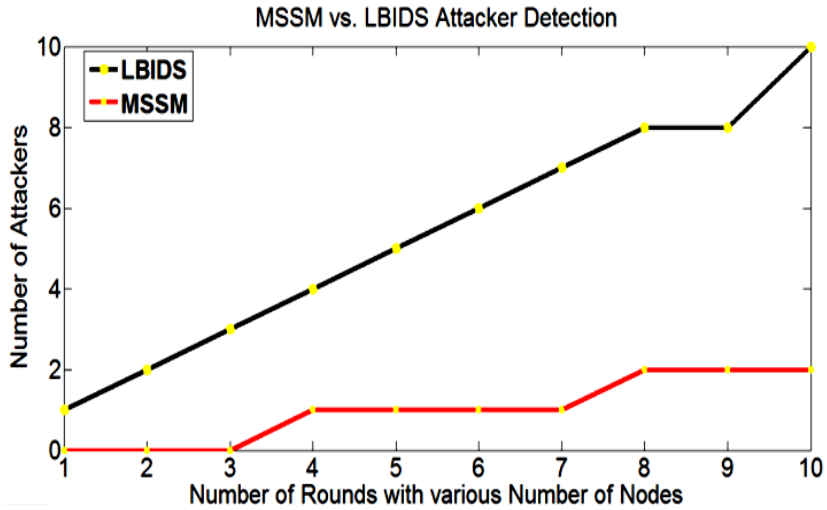

Figure 5: MSSM vs. LBIDS Comparison In-terms of Attacker Detection

The number of attackers detected in each round of the simulation in MSSM is compared with LBIDS as shown in Fig.5. From Fig.5 it is clear that the number of attackers is controlled and less number of attackers detected in MSSM than in LBIDS.

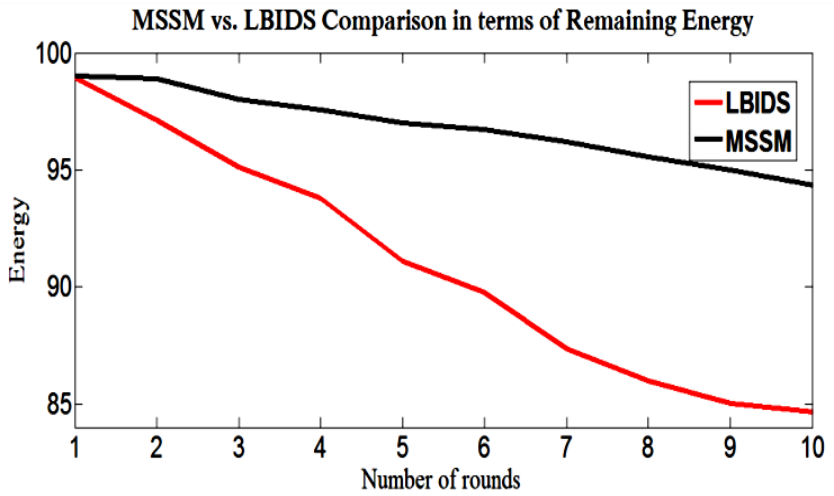

Figure 6: MSSM vs. LBIDS Comparison In-terms of Remaining Energy

The energy consumption in a network depends on the number of packets and the size of the packets transmitted and received in the network. Each node spends some energy to every stage during their life cycle. The energy spends by MSSM is less than the LBIDS as shown in Fig.6. From figure-7 it is clear that the throughput obtained using MSSM is more than the existing system LBIDS. The throughput is the number of successful packet transmissions in the network. The load is the data size and the number of packets with the packet size. Each load depends on the data size transmitted from the source node to a destination node in a route. The energy consumption in a network completely depends on the number of nodes and number of transactions among the nodes. Some of the nodes only transmit the data packets, while some only receive data packets. Some of the nodes are idle whereas others do both transmit and receive.

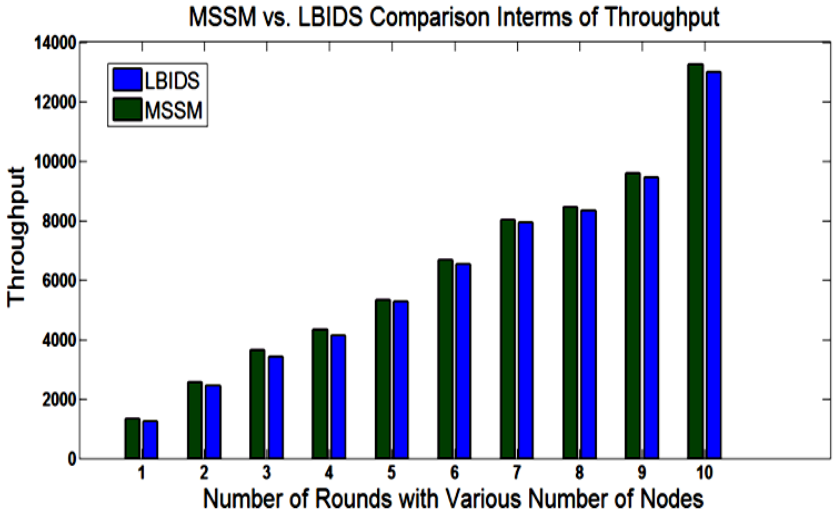

Figure 7: MSSM vs. LBIDS Comparison In-terms of Throughput

In this research the consuming energy depends on the number of nodes. Once the number of nodes is increased by the network, the saving energy decreases and is clearly shown in Fig.8. The number of nodes deployed in the network is changed and the remaining energy is computed.

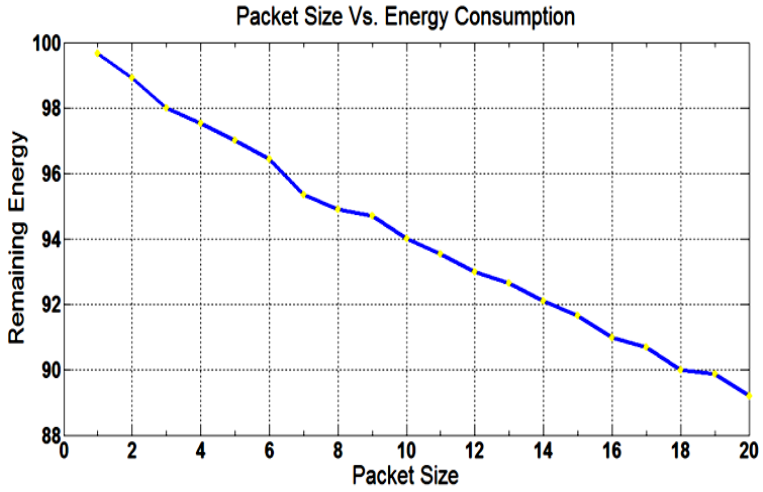

Figure 8: MSSM Performance Comparison Energy In-order to Number of Nodes

The performance of the MSSM is compared with the existing approaches as well as by more number of simulations. In each simulation the numbers of nodes are changed and verified the remaining energy, throughput and the delay of the network. The numbers of nodes deployed in the network are 20, 40, 60, 80 and 100. Fig.9 says that the MSSM saves the time, energy and provides more throughputs with Finite Automate based state activation and deactivation.

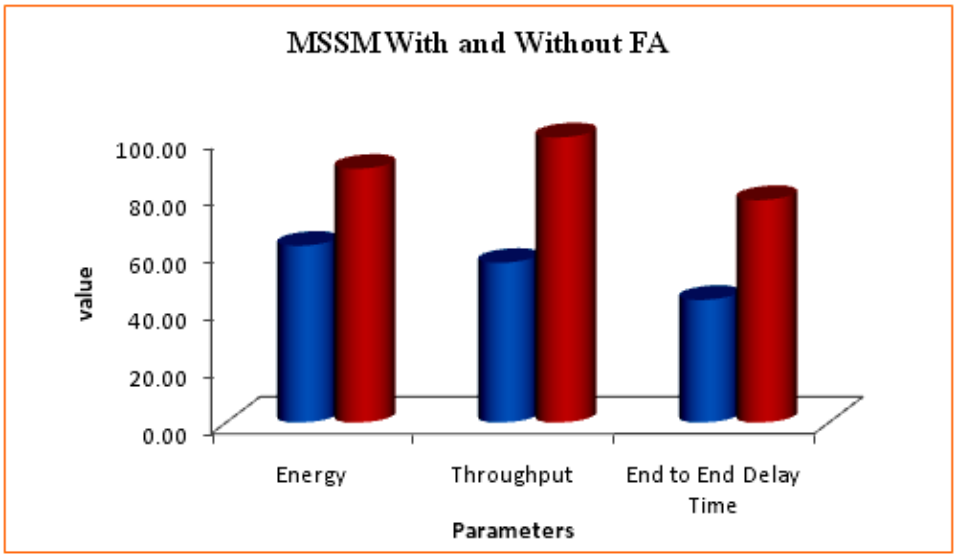

Figure 9: MSSM With and Without FA

Conclusion

This paper discusses and proves that MSSM approach provides better security and also improves the Quality of service in WSN. The attacker node is mostly thwarted using this mechanism. Also the malicious node can be detected in any one of the stages and each stage concentrates on verifying the node behavior and data transmission functionality. MSSM also saves energy due to fewer nodes in the shortest route, less delay due to fast and short distance between nodes. Due to fast, trust-able nodes and shortest path the quality of service is maintained and the attacker node is avoided.

References

[1]. UdayaSuriya Rajkumar, D. and Rajamani Vayanaperumal.: 'A Leader Based Monitoring Approach for Sinkhole Attack in Wireless Sensor Network', 2013 Science Publications.

[2]. Ananda Krishna B, R.Ramesh, "Improving Quality of Service Through Secured Routing In Mobile Ad Hoc Networks", Int. J. Advanced Networking and Applications Volume: 03, Issue: 04, Pages:1253-1260 (2012).

[3]. Yih-Chun Hu, David B. Johnson, "Securing Quality-of-Service Route Discovery in On-Demand Routing for Ad Hoc Networks", ACM, *SASN'04,* October 25, 2004.

[4]. PuneetSethi, GautamBarua, "CRESQ: Providing QoS and Security in Ad hoc Networks",2014.

[5]. S. Chen, "Routing Support for Providing Guaranteed End-to-End Quality-of-Service", PhD Thesis, University of IL at Urbana-Champaign, 1999.

[6]. S. Chakrabarti and A. Mishra, "QoS issues in ad-hoc wireless networks", IEEE Communication. Mag., vol.39,pp. 142-148, Feb. 2001.

[7]. J.N. Al-Karaki and A.E.Kamal, "Quality of Service routing in mobile ad hoc networks: Current and future trends in Mobile Computing", Handbook, CRC Publishers, 2004.

[8]. T.B.Reddy I.Karthigeyan, B.Manoj and C.S.R.Murthy, "Quality of service provisioning in ad hoc wireless networks: a survey of issues and solutions", Ad Hoc Networks Vol.4, pp.83-124, 2006

[9]. L. Chen, W. B. Heinzelman, "QoS-Aware Based on Bandwidth Estimation for Mobile Adhoc Networks", IEEE Journal on Selected Areas in Communications, Vol. 23, No. 3, 561-572, 2005.

[10]. H. Zhu, G. cao, A. Yener and A. D. Mathias, "EDCFDM: A Novel Enhanced Distributed coordination Function for Wireless Ad Hoc Networks", IEEE International Conference on Communications (ICC), Paris, France, June 2004.

[11]. IEEE 802.11-2012, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications", IEEE Standard 802. 11-2012, 2012.

[12]. Daewon Jung 1, Ryangsoo Kim, Hyuk Lim, "Power-saving strategy for balancing energy and delay performance in WLANs", Elsevier -2014.

[13]. L.M. Feeney, M. Nilsson, "Investigating the energy consumption of a wireless network interface in an ad hoc networking environment", in: Proceedings of IEEE Infocom, 2001, pp. 1548–1557.

[14]. K.-C. Ting, H.-C. Lee, H.-H. Lee, F. Lai, " An idle listening-aware energy efficient scheme for the DCF of 802.11n", IEEE Trans. Consumer Electronics 55 (2) (2009) 447–454.

[15]. H. Lin, S. Huang, R. Jan, "A power-saving scheduling for infrastructure-mode 802.11 wireless LANs", Computer Communication. 29 (17) (2006) 3483–3492.

[16]. Y. Agarwal, R. Chandra, A. Wolman, V. Bahl, K. Chin, R. Gupta, "Wireless wakeups revisited: energy management for VoIP over Wi-Fi smart phones, in: Proceedings of ACM Mobi Sys", 2007, pp. 179–191.

[17]. W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure Friend Discovery in Mobile Social Networks," Proc. IEEE INFOCOM, pp. 1647-1655, 2011.

[18]. X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "Seer: A Secure and Efficient Service Review System for Service-Oriented Mobile Social Networks," Proc. IEEE 32nd Int'l Conf. Distributed Computing Systems (ICDCS), pp. 647-656, 2012.

[19]. Masanori Bando, N. Sertac Artan, and H. Jonathan Chao," Scalable Look ahead Regular Expression Detection System for Deep Packet Inspection", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 20, NO. 3, JUNE 2012.