FBMT: Fuzzy Based Merkle Technique for Detecting and Mitigating Malicious Nodes in Sensor Networks

Ranjeeth Kumar Sundararajan[1] and Umamakeswari Arumugam[2]
[1]Department of Computer Science and Engineering, Srinivasa Ramanujan Centre, SASTRA Deemed University, India
[2]Department of Computer Science and Engineering, School of Computing, SASTRA Deemed University, India

Abstract: *Wireless sensor networks are prone to many vulnerabilities because of its unattended environment policy. Intrusion is one of the serious issue in wireless networks, since wireless networks are resource constrained and devising a security mechanism to counter intrusion is a challenging task. This paper focuses on building light-weight Intrusion Detection System to counter the routing attack, by identifying the malicious nodes at the earliest point. The proposed scheme namely Fuzzy Based Merkle Technique applies fuzzy logic to identify the malicious nodes and builds a light-weight Intrusion detection system and adapts Merkle tree approach for building the network. The proposed scheme is efficient in identifying the malicious nodes with minimum energy consumption and less communication overhead than the existing Merkle technique. Network Simulator 2 is used to simulate the Intrusion Detection System (IDS) and the results are verified.*

Keywords: *Wireless Sensor Networks, Intrusion Detection Systems, Fuzzy logic, Merkle tree.*

Received August 12, 2016; accepted October 2, 2018

1. Introduction

Wireless Sensor Networks (WSN) are resource limited environment, in which the sensor nodes are scattered in the field. WSN is a kind of ad hoc network, which can be deployed in the remote environment like battle fields, forest, and so on. Since, the human intervention is not possible in many places, the sensor nodes are deployed for monitoring purposes. So, the security of the sensor network is the vital criteria for successful network deployment. In Denial of Service (DoS) attacks, the intruders restrict the service of particular node or a part of the network to other nodes and create serious damages to the WSN. Many security mechanisms exists to counter the vulnerabilities of the sensor network, like cryptographic mechanisms, key management techniques, Intrusion detection systems and so on. Designing a light-weight IDS for WSN is a challenging task, since identifying the malicious nodes needs excessive computation. This paper focuses on building a light-weight IDS to counter the sinkhole attack in WSN.

1.1. Vulnerabilities of WSN

This paper focuses on the most vulnerable DoS attack namely sinkhole attack, which utilize the routing vulnerability of the network. In this type of attack, the malicious nodes which act as the sinkhole node attracts the entire traffic towards itself and either drops or selectively forwards the packets. Many other routing vulnerabilities exist in WSN, in that sinkhole attack is one of the major threat to the network. So, an efficient security mechanism is essential to counter the sinkhole nodes. The Fuzzy Logic System (FLS) based intrusion detection model is proposed to identify the malicious nodes and alert the network. Even though, many vulnerabilities exist in the WSN environment, the routing attacks causes more performance degradation [17]. So, the predominant routing attack namely sinkhole attack is dealt in this research work.

The security attacks are classified as Active and Passive. The active attacks are the security violations, which makes some changes like altering the information or deleting the information in the transmission. The passive attacks does not make any changes in the transmission, but monitors the transmission between the nodes without their authorization. Some of the active attacks include, Sinkhole attack, Wormhole attack, Sybil attack, Gray-hole attack and so on. Some of the passive attacks are Transmission overhearing or Eavesdropping, Traffic analysis, Camouflage adversaries and so on. Table 1 list few of the layer-wise security attacks in the WSN. This paper focuses on most vulnerable routing layer attack namely, sinkhole attack.

Table 1. Security Attacks.

Layer	Threats
Physical	Jamming, Tampering
Data Link	Collision, Exhaustion, Unfairness
Network	Sinkhole, Worm-hole, Selective forwarding
Transport	Flooding, False Messages, De-synchronization
Application	Reliability attack, Clock Skewing, Data aggregation distortion

1.2. Security Mechanisms in WSN

The Existing security methods to protect the wireless sensor network can be classified into two types, Low-level and High-level methods. The high-level schemes include the Intrusion Detection System, secure data aggregation and key management and so on.

1.2.1. Intrusion Detection System

Intrusion detection system is considered to be the second line of defence to protect the systems [4]. Generally there are three types of IDS, they are classified as below:

1. Signature-based IDS: The set of attack patterns is stored as the signatures. If, the observed behaviour matches with the signatures, then the IDS raises alarm of the malicious activity. This method is also called as the misuse-based or knowledge based and detects the known attacks.
2. Anomaly-based IDS: The normal behaviour of the system or network is stored and if the observed traffic or audit data deviates from the normal pattern, then the IDS alarms the network for occurrence of the malicious activity. This method is also known as behaviour based IDS and it is capable to detect the unknown attacks.
3. Specification-based IDS: The normal behaviour of the system is developed as the specification manually. When, there is a deviation from the normal behaviour, the state changes from normal to malicious and the IDS alarms the network. This method is also known as Stateful Protocol Analysis (SPA) and it is capable to identify the known and unknown attacks with minimum false positive ratio and can be applied to machine critical systems [12]. This research work focuses on building fuzzy based IDS to counter the routing attack, namely sinkhole attack in tree based routing scheme which follows the Merkle tree approach. In [2, 13], various intrusion detection and prevention methods for detecting sinkhole attack is discussed.

This paper is organized as follows: section 2 gives the recent related works in the IDS for WSN, section 3 gives the research background, section IV provides the proposed Fuzzy based IDS algorithm, section 4 provides the simulation results and analysis and section 5 gives the conclusion and future work.

2. Related Works: A Brief Overview

This section demonstrates some of the works present in the literature for intrusion detection model on the WSN. In [4], the author introduces a high level mechanism of securing the network namely IDS which forms the second level of defense for a network. The authors in [8] gives an extensive analysis of the existing IDS methods by classifying them based on the approach, location and so on. The fuzzy set theory is introduced by Zadeh [20] for dealing the uncertainty problems. This fuzzy approach is used in control systems and in many decision making domains. In [16], the authors proposes cross layer detection model for wireless networks and in their method the computation is relatively high which may not be suitable for WSN. The authors in [15] proposes FLS to detect the faulty nodes in WSN. They had shown only energy consumption parameter to evaluate the proposed work and that is not sufficient to analyze the efficiency of the proposed method. In [7], the authors propose specification based IDS for ad hoc environment. The IDS is active throughout the entire network process, so the network performance is degraded. The authors in [18] follows the specification based model to monitor the Ad hoc On-Demand Distance Vector routing (AODV) network. This model incurs more communication overhead due to many message transmissions. Merkle tree based time stamped algorithm is proposed as an authentication scheme against pre image attack [14]. In [9], the authors classifies the detection mechanisms of the sinkhole attack into four categories. The detection methods includes Hop count based detection, Agent based detection, Cryptography based detection and Sequence number based detection.

3. Research Background

3.1. Merkle Tree Scheme

This research paper applies the Merkle tree principle [16] for performing information security. Ralph Merkle invented the concept of Merkle tree or hash tree for secure verification of the messages during the transmission. In this tree, the non-leaf node consist of the hash of the values present in the leaf node. This scheme uses one public key to sign many messages, and the possible number of messages is $N = 2^N$. Figure 2 shows an example Merkle tree which generate public keys X_i and private keys Y_i of 2n. The hash value is calculated as follows:

For each private key $Y_{i,}$ $1 <= i <= 2n$

$$h_i = H(Y_i) \quad (1)$$

The node in the Merkle tree is denoted by a_{ij} where i denotes the level of a node, j denotes the number of the node and h_i denotes the leaf node of the Merkle tree. The inner node of the hash tree is the concatenated

hash value of its child nodes. From Figure 2, the hash value is:

$$a_{1,0} = H(a_{0,0} \,||\, a_{0,1}) \quad (2)$$

$$a_{2,0} = H(a_{1,0} \,||\, a_{1,1}) \quad (3)$$

The root value of the tree $a_{n,0}$ is the public key (pub) generated and this value is verified during the transmission and if there is any change in the pub, then there exist some malicious activity. This research work applies Merkle tree for message verification in the ad hoc routing environment.

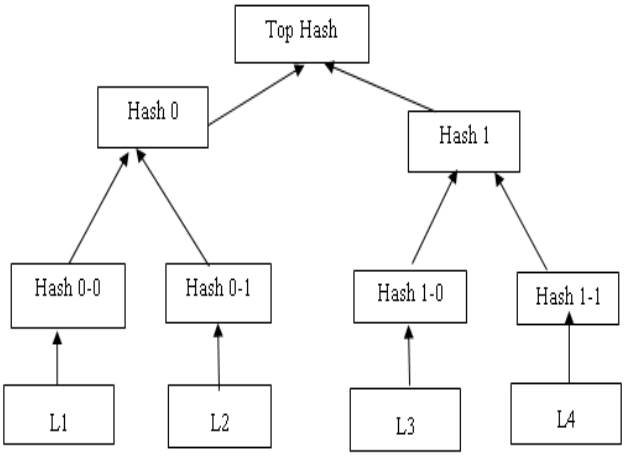

Figure 1. Merkle tree.

3.2. Fuzzy Model

This paper proposes a fuzzy based approach to identify the malicious node in the network. Fuzzy logic is the multi-valued logic obtained from the fuzzy set theory and the probability value ranges from 0 to 1 [19]. The fuzzy set [20] theory is applied to evaluate the truthfulness of the nodes in the network. Figure 3 gives the general architecture of FLS. The crisp inputs from the input variables is applied to the fuzzy engine to create the fuzzy sets, and this process is called as fuzzification [5].

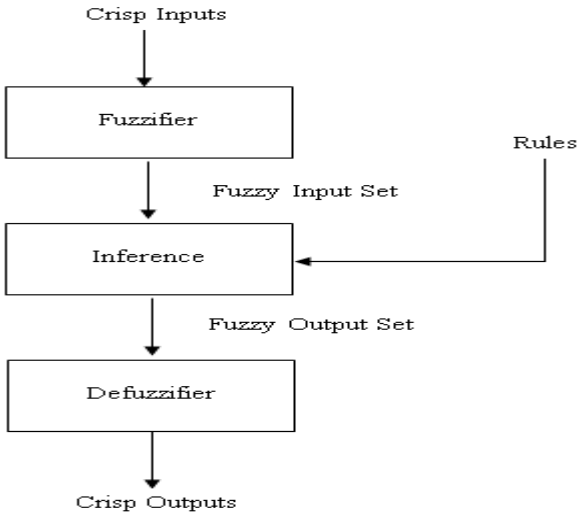

Figure 2. Fuzzy logic system.

The fuzzified values are given as the input to the propositions or rules like IF-THEN to solve the control problem [17] which produce a fuzzified output value. This value indicates the trust value of the sensor node and is applied to the defuzzification module to get the non-fuzzy output. The proposed fuzzy trust model produces the estimated trust value and its relation with the trust threshold determines the trustworthiness of a node.

3.3. Research Motivation

Merkle approach [16] applies centralized security evaluation scheme, in which the top node or root node of the hash tree plays a major role. During the transmission between two entities, the root value or hash value is verified, if it is altered, then the transmission is identified as malicious. In this method, identifying the malicious nodes is difficult because the intruders may exist as an intermediate node or the source. The existing scheme [1] doesn't provide suitable differentiation scheme to identify the malicious node. Also, the root value can easily altered by the intruders, which makes this method less secure. So, this shortcomings of existing scheme motivates to develop strong IDS with less resource consumption. The proposed scheme applies fuzzy logic to identify the malicious nodes with minimal resource consumption.

4. System Design

4.1. System Architecture

The energy value and trust value are the linguistic variables to the fuzzy system. These variables are decomposed to the linguistic terms.

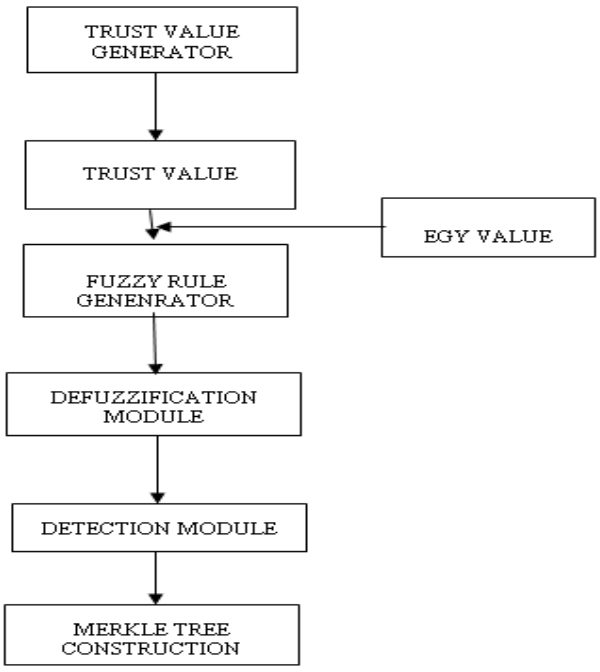

Figure 3. IDS architecture.

- *Energy Variable:*

Let the energy (egy) is the linguistic variable which represents the energy value of the nodes in the network. To qualify the linguistic values of the energy, terms such as "*low*" and "*high*" are used. These are the linguistic values to the energy. Then, the following equation gives the set of decomposition (*E*) for the linguistic variable energy.

$$E(e) = \{very\text{-}low, low, medium, high, very\text{-}high\} \quad (4)$$

- *Trust variable:*

Let the trust (spd) is the linguistic variable which represents the trust value from the physical layer of the network. To qualify the linguistic values of the trust, terms such as "*low*" and "*high*" are used. These are the linguistic values to the trust. Then, the following equation gives the set of decomposition (*T*) for the linguistic variable trust.

$$T(t) = \{very\text{-}low, low, medium, high, very\text{-}high\} \quad (5)$$

Algorithm 1: EnergyInput ( )

{Let egy be the input energy to the fuzzy system, EGY_HI be the optimal value of energy, EGY_LOW be the lower value of energy

If (egy > EGY_HI) Return HIGH;

Else if (egy< EGY_LOW) Return LOW;

Else Return MEDIUM;}

Algorithm Description: The energy is given as the input to the fuzzy system and if, the value is higher than the given optimal value, the fuzzy system responds with energy high value. If, the energy value is less than the given optimal value, the fuzzy system responds with energy low value or else the energy medium value.

Algorithm 2: TrustInput ( )

{Let spd be the input trust value to the fuzzy system which is received from the physical layer, TRUST_HI be the optimal value of trust, TRUST_LOW be the lower value of trust

If (spd > TRUST_HI) Return HIGH;
Else If (spd < TRUST_LOW)
Return LOW;
Else Return MEDIUM;}

Algorithm Description: The trust is given as the input to the fuzzy system from the wireless physical layer and if, the value is higher than the given optimal value, the fuzzy system responds with trust high value. If, the trust value is less than the given optimal value, the fuzzy system responds with trust low value or else the trust medium value.

Algorithm 3: Fuzzyrule ( )

Algorithm Description: Fuzzification process obtains the fuzzy set using fuzzy linguistic variables, fuzzy linguistic terms and membership functions. Table 2 list the fuzzy rules applied.

Table 2. Fuzzy rules.

n_1(egy)	n_2 (spd)	Result
Low	Low	Very Low
Low	Medium	Low
Low	High	High
Medium	Low	Very low
Medium	Medium	Low
Medium	High	Medium
High	Low	Very low
High	Medium	High
High	High	Very high

Algorithm Description: Let n_1, n_2 denote the input linguistic variables given to the fuzzy inference engine, where n_1 denotes the energy and n_2 denotes the trust from the physical layer. The fuzzy rule is applied to identify the node trust value with the application of fuzzified energy and trust values. The values are evaluated based on the combination of the n1 (energy) and n2 (trust) values. The fuzzy engine generates the results based on the combinations of the input values and the result is sent as an input for the defuzzification process.

Algorithm 4: Defuzzification ( )

{ If (rule=LOW) Return (0, LOW)
If (rule=MEDIUM) Return (LOW, MEDIUM)
If (rule=HIGH) Return (MEDIUM, HI)
If (rule=VERYHIGH)
Return (HI, VERYHIGH)
Return (0, 1)}

Algorithm Description: Defuzzification is the process of transferring the aggregated fuzzy output to a crisp output value [3]. The defuzzification module transfers the fuzzified trust value to normal trust value. If the fuzzy rule generates LOW as output, then the IDS randomly generates the trust value and it is returned. Similarly, the IDS return random values for MEDIUM, HIGH, and VERY HIGH and so on. The final trust value (Tvalue) is returned in the interval of [0, 1].

Algorithm 5: Detection ( )

{Get Tvalue from the defuzzification module,
Let Trust_Threshold = 0.4;
If (Tvalue <= Trust_Threshold)
{Add the Node ID to the malicious list and broadcast the Node ID. Remove the Malicious node from the tree….
Start new Merkle tree formation.}}

Algorithm Description: The trust value of the member nodes is extracted from the defuzzification module. Consider the following scenario:
th = 0.4 // th - Trust threshold

Consider two states.
State 1: tv < th // tv - Trust value
State 2: tv > th

State 1 indicates the trust value of the nodes are less than the trust threshold, then the node may be a malicious node and added to the list namely malicious list. State 2 indicates that trust value equals or higher than the trust threshold, that indicates the nodes are

genuine. The node ID of the malicious node is broadcasted to the neighbor nodes and removes the malicious node from further routing process.

5. Simulation and Analysis

The proposed work namely Fuzzy Based Merke Tree (FBMT) was simulated in NS2 (Network Simulator 2) and the performance is compared with the existing scheme Merkle Tree (MT) [1] using metrics like energy consumption, packet drop rate, packet delivery ratio and throughput is analysed in two different scenarios which include varying the packet interval and varying the node density.

Table 3 shows the simulation setup. The assumptions for the simulation is listed below:

1. BS has the highest energy resource.
2. All the sensor nodes are static.

Table 3. Simulation setup.

Sensor Nodes	50
Base Station	1
Initial Energy	100 J
EGY_LOW	0.3
EGY_HIGH	0.7
TRUST_LOW	0.5
TRUST_HIGH	0.8

5.1. Varying Packet Interval

1. Average Energy Consumption

Figure 4 depicts the ratio of the energy consumed by the sensor nodes to the total energy consumption that gives the average energy consumption. The proposed work FBMT consumes less power compared to the existing Merkle tree scheme MT by varying the packet interval. The proposed FBMT consumes 3% less energy compared to the existing MT scheme. In Table 4, the results are given in the tabular format.

Table 4. Average Energy Consumption values.

Interval / Scheme	0.1	0.2	0.4
MT	0.707072	0.274121	0.214299
FBMT	0.689317	0.25806	0.199889

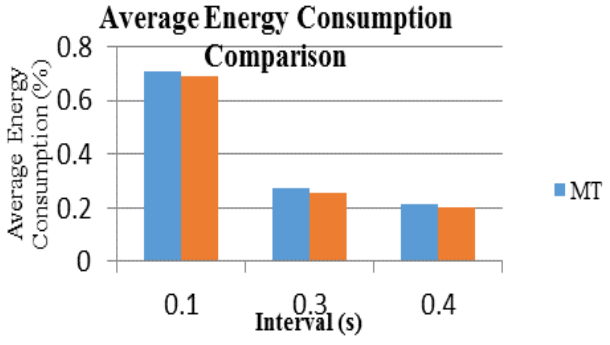

Figure 4. Average energy consumption.

2. Packet Drop Ratio

Table 5 gives the packet drop ratio values obtained by simulation. Figure 5 depicts the ratio of the difference between the number of packets sent and received gives the packet drop ratio. The proposed work FBMT has less number of packet drop ratio compared to the existing Merkle based scheme MT by varying the packet interval. The proposed FBMT consumes 24% less packet drop ratio than the existing MT scheme.

Table 5. Packet drop ratio values.

Interval / Scheme	0.1	0.2	0.3	0.4
MT	35.4155	3.47448	6.35179	6.08696
FBMT	32.1021	2.17155	4.07166	5.21739

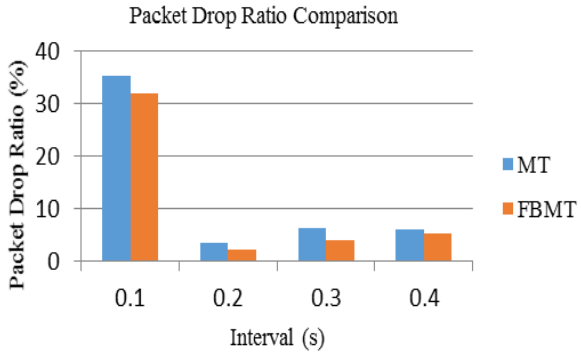

Figure 5. Packet drop rate comparison.

3. Packet Delivery Ratio

Table 6 gives the packet delivery ratio obtained during simulation. Figure 6 depicts the ratio of the received packets and the packets sent and gives the packet delivery rate. The proposed work FBMT has highest number of packets delivered to the destination compared to the existing Merkle based scheme MT by varying the node density. The proposed FBMT scheme 2.5% higher delivery ratio than the existing MT scheme.

Table 6. Packet Delivery Ratio values.

Interval / Scheme	0.1	0.2	0.3	0.4
MT	64.5845	96.5255	93.6482	93.913
FBMT	67.8979	97.8284	95.9283	94.7826

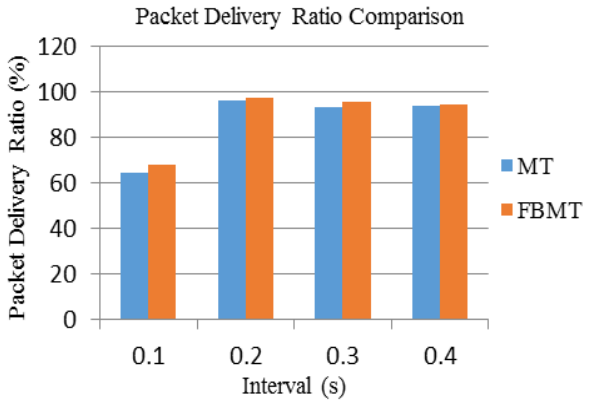

Figure 6. Packet delivery ratio comparison.

5.2. Varying Node Density

5.2.1. Detection Ratio

Figure 7 gives the ratio of the detected compromised nodes. The proposed FBMT scheme achieves around 95% higher detection rate, which is 55% higher than the existing MT scheme.

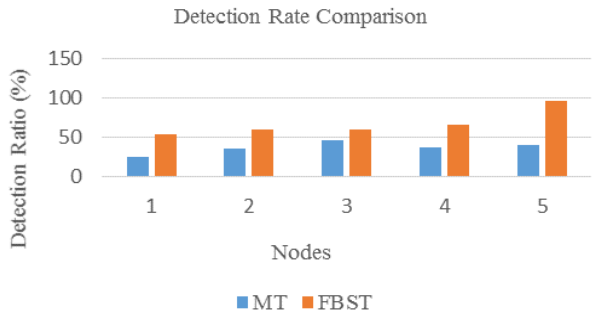

Figure 7. Detection rate comparison.

5.2.2. Packet Delivery Ratio

Figure 8 depicts the ratio of the received packets and the packets sent that gives the packet delivery rate. The proposed work FBMT has highest number of packets delivered to the destination by 22% higher compared to the existing Merkle based scheme MT by varying the node density.

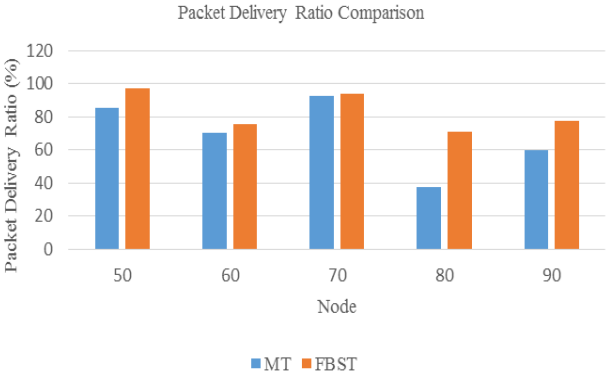

Figure 8. Packet delivery ratio consumption.

5.2.3. Packet Drop Ratio

Figure 9 gives the ratio of the difference between the number of packets sent and received. The proposed work FBMT has 43% less number of packet drop ratio compared to the existing Merkle based scheme MT.

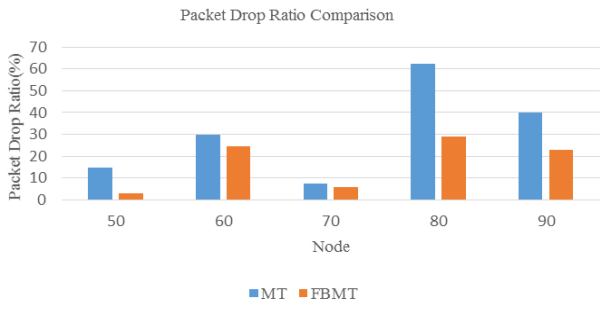

Figure 9. Packet drop ratio comparison.

5.2.4. Throughput

Figure 10 shows the throughput comparison which is the ratio of the total packets received to the certain period of time. The proposed scheme FBMT has 23% higher throughput compared to the existing scheme MT in terms of varying node density.

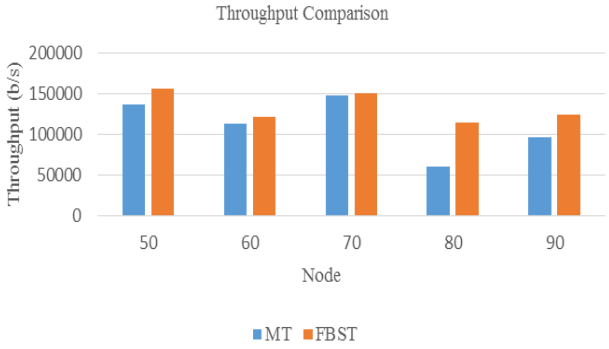

Figure 10. Throughput comparison.

6. Conclusions and Future Work

Wireless sensor networks is vulnerable to many threats because of its nature of deployment. The existing method MT adapts Merkle signature scheme for validation of a node. The proposed FBMT scheme applies fuzzy rules to identify the malicious node with minimum resource consumption like less energy, less overhead, less packet drop ratio and higher packet delivery ratio, throughput than the existing Merkle based scheme. In future, this work will be extended by applying generic specification based IDS model to verify the malicious behavior of a node and also this work can be extended to the Internet of Things environment.

Acknowledgment

The authors would like to acknowledge SASTRA University for the great support and assistance rendered to carry out this research work.

References

[1] Baadache A. and Belmehdi A., "Fighting Against Packet Dropping Misbehavior in Multi-Hop Wireless Ad Hoc Networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 1130-1139, 2012.

[2] Bhatiya A., Tilwankar A., Lambhate D., and Kumar K., "Detection and Prevention of Sink Hole Attack in AODV Protocol for Wireless Sensor Network," *International Research Journal of Engineering and Technology*, vol. 4, no. 5, pp. 2192- 2201, 2017.

[3] Chandran K., Shanmugasudaram V., and Subramani K., "Designing a Fuzzy-Logic Based Trust and Reputation Model for Secure Resource Allocation in Cloud Computing," *The*

International Arab Journal of Information Technology, vol. 13, no. 1, pp. 30-37, 2016.

[4] Denning D., "An Intrusion-Detection Model," *IEEE Transactions on Software Engineering*, vol. 13, no. 2, pp. 222-232, 1987.

[5] Goztepe K., "Designing a Fuzzy Rule Based Expert System for Cyber Security," *International Journal of Information Security Science*, vol. 1, no. 1, pp. 13-19, 2012.

[6] Gronkvist J., Hansson A., and Skold M., "Evaluation of a Specification-Based Intrusion Detection System for AODV," *in Proceedings of 6th annual Mediterranean Ad Hoc Networking Workshop*, Corfu, pp. 121-128, 2007.

[7] Javanmardi S., Barati A., Dastgheib S., and Attarzadeh I., "A Novel Approach for Faulty Node Detection with the aid of Fuzzy Theory and Majority Voting in Wireless Sensor Networks," *International Journal of Advanced Smart Sensor Network Systems*, vol. 2, no. 4, 2012.

[8] Liao H., Lin C., Lin Y., and Tung K., "Intrusion Detection System: A Comprehensive Review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16-24, 2013.

[9] Mathew A. and Terence S., "A Survey on Various Detection Techniques of Sinkhole Attacks in WSN," *in Proceedings of the IEEE International Conference on Communication and Signal Processing*, Chennai, pp. 1115-1119, 2017.

[10] Merkle R., "A Digital Signature Based on a Conventional Encryption Function," *in Proceedings of Advances in Cryptology-CRYPTO'87*, Santa Barbara, pp. 369-378, 1987.

[11] Raja S. and Ramaiah S., "Performance Comparison of Neuro-Fuzzy Cloud Intrusion Detection Systems," *The International Arab Journal of Information Technology*, vol. 13, no. 1A, pp. 142-149, 2016.

[12] Ruschitzka K. and Levitt K., "Execution Monitoring of Security-Critical Programs in Distributed Systems: A Specification-based Approach," *in Proceedings of IEEE Symposium on Security and Privacy*, Oakland, pp. 175-187, 1997.

[13] Santhi G. and Sowmiya R., "A Survey on Various Attacks and Countermeasures in Wireless Sensor Networks," *International Journal of Computer Applications*, vol. 159, no. 7, pp. 7-11, 2017.

[14] Sharma K. and Vairamuthu S., "Enhancing The Security Through the Usage of Merkle Tree and Timestamp in Peer to Peer Messaging," *International Journal of Pure and Applied Mathematics*, vol. 119, no. 7, pp. 13-20, 2018.

[15] Siddiqui S., Khan P., and Khan M., "Fuzzy Logic Based Intruder Detection System in Mobile Ad hoc Network," *Bharati Vidyapeeth's Institute of Computer Applications and Management International Journal of Information Technology*, vol. 6, no. 2, pp. 767-773, 2014.

[16] Singh J., Kaur L., and Gupta S., "A Cross-Layer Based Intrusion Detection Technique for Wireless Networks," *The International Arab Journal of Information Technology*, vol. 9, no. 3, pp. 201-207, 2012.

[17] Sundararajan R. and Arumugam U., "Intrusion Detection Algorithm for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Networks," *Journal of Sensors*, vol. 2015, 2015.

[18] Tseng C., Balasubramanyan P., Ko C., Limprasittiporn R., Rowe J., and Levitt K., "A Specification-based Intrusion Detection System for AODV," *in Proceedings of the 1st ACM workshop on Security of Ad hoc and Sensor Networks*, Washington, pp. 125-134, 2003.

[19] Yu Y., Li K., Zhou W., and Li P., "Trust Mechanisms in Wireless Sensor Networks: Attack Analysis and Countermeasures," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 867-880, 2012.

[20] Zadeh L., "Fuzzy Sets," *Information and Control*, vol. 8, pp. 338-353, 1965.

Ranjeeth Kumar Sundararajan started the basic degree in computer science in Jawahar Science College, Neyveli, Tamilnadu, India. He completed his Master degree in computer technology from Coimbatore Institute of Technology, Coimbatore, Tamilnadu, India and a Master degree in computer science and engineering from Pavendar Bharathidasan College of Engineering and Technology, Trichirappalli, Tamilnadu, India. He had completed his Ph.D in the field of Wireless Sensor Networks from SASTRA Deemed University. He has 5.5 years of teaching experience in engineering institutions and participated in several conferences and workshops. He published one research paper in international conference and participated in young IT professional competition conducted by CSI India. He is currently working as an Assistant Professor in the department of Computer Science & Engineering, Srinivasa Ramanujan Centre, SASTRA Deemed University, Kumbaonam, Tamilnadu, India. His research interests are Network Security, Wireless Sensor Networks, Cloud Computing, Internet of Things and Objected Oriented Design.

Umamakeswari Arumugam received her Bachelor's degree in Engineering from A.C.C.E.T., Karaikudi in 1989, Master's Degree in 1994 from NIT (formerly REC), Trichy and Doctorate from SASTRA University in 2009. She has 25 years of work experience and her research interests are in the area of Computer Vision, Embedded Systems, Wireless Sensor Networks and Software Engineering. She has presented papers in Conferences and published papers in reputed Journals. She has done collaborative projects and also organized international conferences. She is currently working as Dean, School of Computing, SASTRA Deemed University, Thanjavur- 613401, Tamil Nadu, India.