Measurement 167 (2021) 108272

Contents lists available at ScienceDirect

Measurement

journal homepage: www.elsevier.com/locate/measurement

An intelligent based healthcare security monitoring schemes for detection of node replication attack in wireless sensor networks

S. Anitha [a,*], P. Jayanthi [b], V. Chandrasekaran [c]

[a] Department of Information Technology, Kongu Engineering College, Erode 638060, India
[b] Department of Computer Science and Engineering, Kongu Engineering College, Erode 638060, India
[c] Department of Medical Electronics, Velalar College of Engineering and Technology, Erode 638060, India

ARTICLE INFO

Keywords:
Wireless sensor networks
Wireless body area networks
Replica node
Healthcare monitoring system
Detection probability
Communication overhead
Storage overhead

ABSTRACT

Due to the increased growth of elderly people in recent years, healthcare systems face many challenges on the money spent for those people. Both quality and affordability has to be provided by the new technology which is the today's need. When applying WSN technologies, the advantages such as continuous monitoring with alert mechanisms and relative information are to be satisfied. Among the other challenges, due to the deployed environment, security is a key challenge. As gateway connects to the wireless networks, it is the target area for many adversaries to launch various attacks. Initially, attacker launches node compromise attack which leads to node replication attack. The introduced security methods for intelligent healthcare monitoring system effectively detect replication attack and provide protection to the system. The potential application of proposed methods namely Exponential Moving Average based Replica Detection (EMABRD), Secured Ant Colony Optimization (SACOP) and Fingerprint based Zero Knowledge Authentication (FZKA) is applied to a real time environment. While comparing three algorithms, SACOP has higher detection probability of malicious nodes at the expense of increased storage and communication overheads over EMABRD and FZKA. FZKA performs better compared to EMABRD in terms of detection probability but at the cost of increased overheads. So, among the three algorithms, EMABRD is better in terms of overheads and SACOP is better in terms of detection probability.

1. Introduction

Recent advances in the technologies of WSN have gained attention towards various fields like healthcare, entertainment, industry, retail and travel and emergency management in order to improve the quality of life [1,2]. During recent years, healthcare monitoring system has been paid more attention because of tremendous growth in technology in spite of its security challenge. The performance of WSNs is affected by challenges, potential threats and vulnerabilities of healthcare monitoring system.

Due to the increased growth of elderly people in recent years, healthcare systems face many challenges on the money spent for those people. Both quality and affordability have to be provided by the new technology which is the today's need [3]. When applying WSN technologies, the advantages such as continuous monitoring with alert mechanisms and relative information are to be satisfied. In terms of quality and cost, WSN is one among the possible technologies providing a viable solution.

Moreover, in connecting wearable devices, WSN plays a major role [6]. As the continuous and close monitoring of the individuals provided by wearable devices, flawless health status is maintained. When combining these systems with telemedicine, alert message is generated when an abnormal situation occurs. In order to track the recovery and diagnosis of health issues [29]on long term monitoring, an integrated wearable device [30] is focused. In Kakria et al [4], with such technology, patients with cardiac problems have been monitored successfully.

For various monitoring operations such as drug therapy, knee surgery, and brain trauma rehabilitation, an integrated system is used. For simple pulse monitors, to monitor Holter (an occasionally ambulatory electrocardiography device) and day-to-day activities [5,7], the wearable devices have been used nowadays as indicated in Shanmugam maheswaran et al [3]. Fall detection, location detection and posture detection are some of the applications under focus. To integrate with some substances to embed in the body, research works concentrates in developing tiny sensors recently.

The challenges of static WSN towards healthcare monitoring system

* Corresponding author.
E-mail address: anitha4ciet@gmail.com (S. Anitha).

https://doi.org/10.1016/j.measurement.2020.108272
Received 17 May 2020; Received in revised form 27 June 2020; Accepted 18 July 2020
Available online 25 July 2020

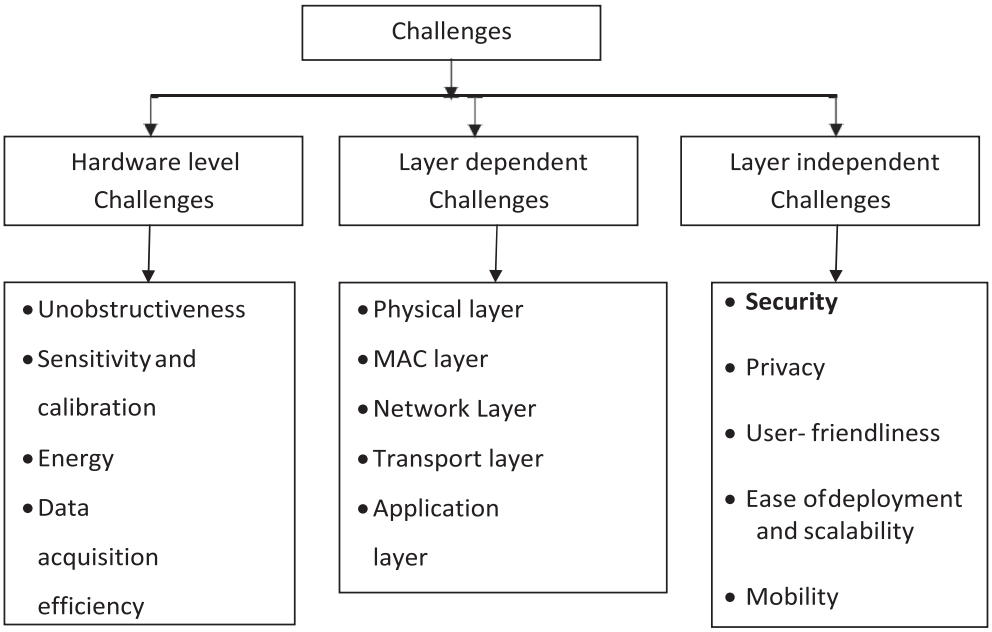

Fig. 1. Various challenges in static WSN when applied to Healthcare Monitoring System.

is on the rise due to its vast applicability. The challenges come in various levels such as from hardware, layer dependent and independent one. Among the other challenges, due to the deployed environment [8], security is a key challenge. As gateway connects to the wireless networks, it is the target area for many adversaries to launch various attacks. Initially, attacker launches node compromise attack which leads to node replication attack. The introduced security methods for intelligent healthcare monitoring system effectively detect replication attack and provide protection to the system. The following are the merits of Healthcare Monitoring System applied as static WSN.

- Monitoring remotely
- Identification in real-time and its actions
- Identification based on context

The static WSN are used in various healthcare applications due to above-mentioned advantages. It include,

- Day-to-day activity monitoring
- Fall and movement detection
- Location tracking
- Medication intake monitoring

The healthcare monitoring system applications pave the way for various issues. The remaining paper sections are sequenced as follows. The existing work is dealt in Section 2. In Section 3, challenges and threats in healthcare monitoring system are given. The architecture and components of healthcare monitoring system is discussed in Section 4. In Section 5, proposed algorithms for healthcare monitoring system are analyzed. Simulation and real-time setup are provided in Section 6. In Section 7, performance evaluation is done. Lastly, Section 8 describes the conclusion.

2. Related work

Medical sensing becomes more popular and widely used by the individuals at hospitals, homes, working and other living places due to the recent advances in microelectronics as denoted by Ko et al [9]. Using healthcare sensors and actuators, reliable and secure IoT based healthcare services are provided to patients and caregivers as indicated in Le et al [10]. In spite, it restricts people to make use of healthcare applications based on IoT because of misuse or privacy. To apply security level demands and system architecture, existing security and protection mechanism cannot be reused because of resource limitation.

Kumar et al [11] provides an architecture which includes several medical sensors, Mica2 motes mounted on board and placed on the patient's body. For further analysis, using medical sensors, the body data of patient's are sensed and transmitted to the end-user devices wirelessly. Using PDA, a query regarding patient health is issued for a doctor or medical professional based on a publish-and-subscribe architecture which is developed by CodeBlue. The relevant data sensed by healthcare sensors are published through an appropriate channel. Upon subscription request by the user, it is viewed through hand-held devices.

Aminian et al. [12] deigned a ubiquitous healthcare prototype system for hospitals. This healthcare system uses unobtrusive wireless sensors for monitoring and communicating patient's health status through PC. Medical monitoring and data access, enhancing memory and communicating with the healthcare provider are the healthcare services provided in case of crisis state through SMS or GPRS. Zhang et al [13] developed mobile health (mHealth) technologies to experience a minor change in direction from wearable sensors in carrying out multifunctional capabilities through smartphone. Uma Gowri et al [14] proposed enhanced collision slot reframing detection protocol for both detecting and preventing cloning attack in wireless body area network.

Mainanwal et al [15] discussed various security requirements and its issues in WBANs. Generally, sensors inserted in the body generate physiological information which may reveal a disease or disability, data confidentiality is a relevant security requirement in BAN systems. Likewise, other security requirements like integrity, availability, authentication (various schemes given in El-hajj et al) [16], authorization must be satisfied. So, a secure BAN architecture should guarantee that data have not been modified during transmission or storage. A property that indicates if the received information is recent and arrives when expected (data freshness) should be evaluated at the personal and external servers to prevent replay attacks.

Ghamari et al [17] designed a Wireless Body Area Networks (WBANs) connected with sensors operated using IEEE 802.15.6 standard. It is used to address needs of low power, low cost, low complexity, high throughput and short-range wireless communication in and around the human body. For remote monitoring with sensor nodes distributed

in a wide area, WBAN with sensors are used unlike WSN [18–19]. Several sensors are placed in clothes, directly on the body or under the skin of a person in order to measure temperature, blood pressure, heart rate, ECG, EEG, respiration rate etc., High reliability is expected in both the sensing and data transmission to save the life of a patient [20]. Performance of these WBANs decreases in high interference scenarios especially in the densely populated areas and in the ISM wireless band.

Sumit et al. [21] designed an IoT technology which provides solution for the difficulty inherent to an aged society. In order to enhance the user's convenience, healthcare and safety, IoT provides control and management of all devices connected via smart home technology in a residential space. The most significant directions for future development of smart homes are the specialization for daily healthcare and provision for super-aged society. Constant monitoring of elderly people is employed through healthcare services with welfare facility liaisons and visiting experts. To rectify this problem, IoT technology is a vital thought satisfying the requirement of constant monitoring of elders automatically. In addition, integrating the IoT technology with the expanded healthcare services allows professionals to get important information other than from medical facilities with less effort. For distinctive purposes, healthcare devices are developed over a period of time. But the limitation is that the data collected by these devices can be used for single purpose only. In order to automatically receive health information, AAL (Ambient Assisted Living) make use of ICT [22]. During their natural daily routine, users monitor health status, improve nutrition and exercise level and learn healthy habits.

To handle node replication attack in sensor networks, replica detection is a widely accepted approach. In addition to developing efficient mechanism for detecting replica node, optimizing the overall network performance is an important one. Thus the performance of the mechanism is evaluated not only based on higher detection probability but also on lower communication and memory overhead. So in this present work, the proposed methods are analyzed using both simulation and real-time experiments and compared its distinctive features.

3. Challenges and threats in healthcare monitoring system

In healthcare perspective, the challenges faced by WSN are generally classified into three categories as denoted in Fig. 1.

Among different challenges, security is an important one in healthcare monitoring system due to the high risk in handling vital data of patients. The various reasons include,

- The network topology becomes large when the sensors are inserted in the patient's body
- Environment is uncontrollable and
- Sensor nodes are resource-limited

The healthcare monitoring system is vulnerable to various security threats and prone to passive or active attacks due to above issues. Node replication attack is a danger one as it paves the way for other types of internal attacks. So, this causes more risk in handling patient's data for maintaining confidentiality and integrity. Also, the replicated device gains unauthorized access into the system thereby gets the authentic (original) patient data.

The system has to provide multi-level security in every part of the network in order to overcome such a type of attack. Even though the proposed security solutions such as key distribution, encryption, public key cryptography and trusted server exist, many drawbacks make the solution at its infant stage. The following are the observations made in the existing security solutions [23].

- Scalability problem incurs in key distribution
- Resource limitation in using public key cryptography
- Single point of failure occurs in the trusted server

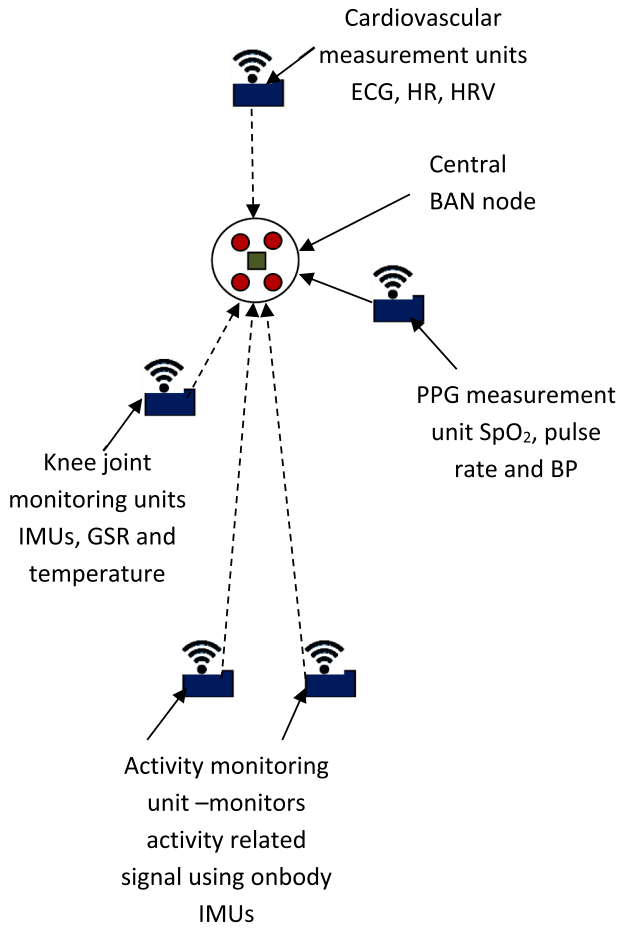

Fig. 2. Different types of sensors inserted in the body and central BAN collects the information.

Therefore, an effective security mechanism overcoming the above-said limitations must be designed providing multi-layer security to the healthcare monitoring system.

4. Architecture and components of healthcare monitoring system

Consider a healthcare monitoring environment consisting of a central Body Area Network (BAN) through which different types of sensors inserted in the body senses and transmits data to the home gateway [24]. Likewise, many central BANs are connected together to send the details sensed by different sensors inserted in the body to the doctor as shown in Fig. 2.

The following are the types of sensors used in WBANs as denoted in Summit et al [21], Ullah et al [25]:

- Accelerometer

To detect acceleration and position of the body relative to freefall in three axes, a device named Accelerometer built based on MEMS technology is used. In order to measure orientation and speed, single and multi-axes devices are used.

- Gyroscope

A type of sensor which measure or maintain the orientation is gyroscope. This rotor sensor works on the principle of conservation of angular momentum. For operating with various gyroscopes such as MEMS, optic fiber, solid state ring lasers and the extremely sensitive

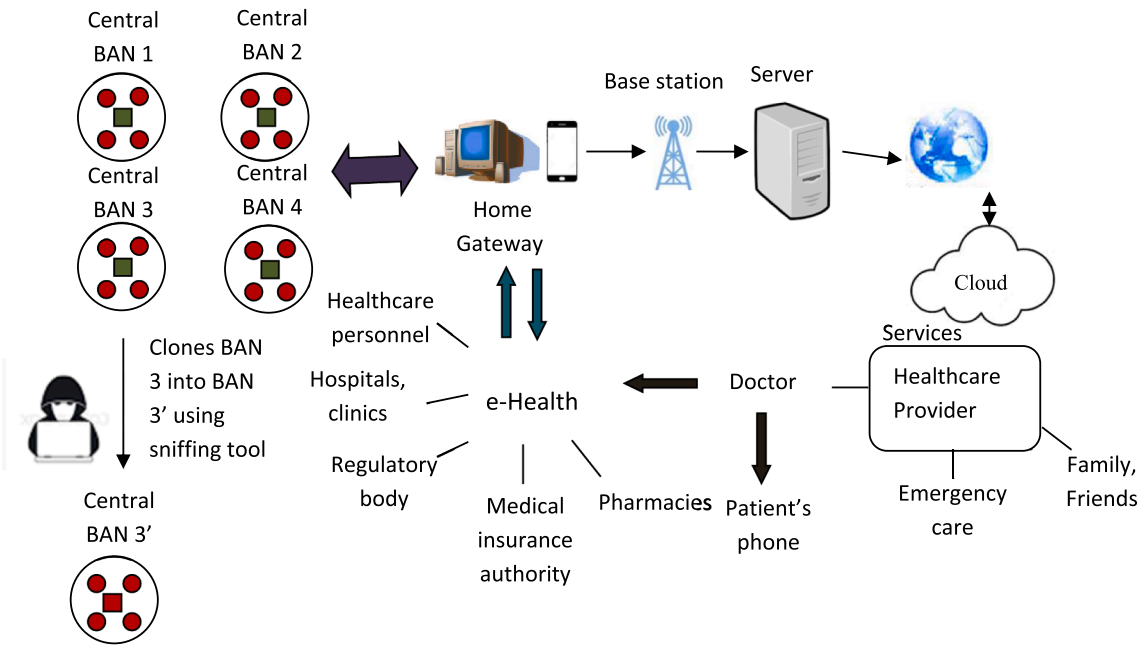

Fig. 3. Healthcare monitoring environment with cloned BAN node.

quantum gyroscope, other principles also exist. Also, to maintain direction in tunnel mining, gyroscopes are used.

- Electrocardiogram (ECG)

While heart contracts, Electrocardiogram receive and record the electrical stimulation. The appearance of an electrical and mechanical activity is determined by electrical stimulation of a muscle cell. ECG signal, Heart Rate (HR), Respiration Rate (RR) and Heart Rate Variability (HRV) are measured using ECG sensor.

- Pulse oximeter

A medical device which is used for monitoring the oxygen saturation of a patient's blood by absorbing the infrared light at the measuring site is called pulse oximeter.

- Blood pressure

The principal vital sign in the body is known through the measurement of blood pressure in the arteries. It increases and decreases more rapidly along the arterioles and small arteries and when the blood moves through the capillaries and back to the heart through veins respectively.

- Photoplethysmogram (PPG)

To determine the arterial oxygen saturation (SpO_2) level, PPG signal is used. By measuring and comparing the intensity of transmitted light at two wavelengths, SpO_2 is calibrated from the PPG signal. PPG also determine respiration rate, pulse and heart rates.

- Galvanic Skin Response (GSR)

Change in skin conductivity due to sweating is detected by attaching electrodes on the body surface which is measured using GSR. Also, to perform better assessment of an individual's health condition, GSR level is used.

- Body Temperature (BT)

BT sensor measures body temperature.

Assuming that the adversary captures BAN 3 in Fig. 3, clones it and insert in the network. Although the adversary location is unknown, it is within the transmission range of any one of the BAN. The adversary inserts the cloned node into the network during normal safe mode operation or when the network recovers after depletion state. As the adversary located at remote place, the cloned node reaches the base station through multi hop transmission. Following any path between adversary and base station, cloned node reaches the base station through any of the BAN and home gateway.

The adversary clones the BAN 3 and intrudes into the network through any of the BANs which is in accessible range. In the above case, cloned node BAN 3′ enters the network through BAN 4 as it is in the coverage range of the cloned node and reaches the base station through neighbor or intermediate BAN 2. At a certain point of time, the intermediate nodes or base station receives conflicting information about BAN 3 with same ID and different location. The local verification in which common neighbor or intermediate node receiving information from both BAN 3 and BAN 3′, refuses to forward data and informs base station where global verification is done for revocation of cloned node from the network.

5. Analysis of proposed algorithms in healthcare monitoring system

The existing solution available in the literature only detects and removes cloned node based on ID and its location after verifying with any one or more witness nodes. There may occur two problems viz., if witness is cloned, then major part of the network is under the control of adversary.

5.1. EMA model based energy prediction for replica node detection

The comparison between the energy prediction result and the real energy consumption is made to detect replica nodes using EMA method. To launch replica attack, additional energy is spent by replica nodes. Consequently, if there is significant difference between the energy prediction results and real energy consumption of nodes, multiple identities of replica nodes can be detected. Let $E_c^{'}$ and E_c denote the estimated and actual energy consumption respectively. This method detects the replica

```
Begin
    Initialize trust T, threshold λ, pheromone Δτ_k(t)and energy φ_j(t)
    While end of stopping condition do
      A starting node is positioned with each ant k
      For each node x do
        Calculate the direct T_dir(i,j)and indirect T_ind(i,j) trust values
        if (T^x_total(i,j) > λ)
        Choose next node by applying selection probability p^k_ij(t)
        Apply step by step pheromone update τ_ij(t)
        else
            Remove the node from the path
        End for
      While a solution is built by every ant
      Update with the solution which is best
      Apply updation of offline calculation of pheromone
    End while
End
```

Fig. 4. Pseudocode to detect replica node in optimal path.

node when the following condition is satisfied as given in Eq. (1),

$$\frac{E_c^{'}}{E_c} > Th \tag{1}$$

5.2. SACOP based energy trust system for replica node detection

The trust value of any node is calculated by the recommendation provided by its neighbors. The trust value possessed by the node less than the threshold means the node is said to be malicious which is removed from the network, otherwise the node is considered as the trusted node. The pseudocode in detecting replica node based on SACOP [26] is given in Fig. 4.

5.3. Fingerprint based zero-knowledge protocol for replica node detection

Two-level authentication algorithm [27] solves the above-said problem. First level is that verifying unique fingerprint of each and every node and second level is verifying authenticity of each node without sending the secret value. When BAN 3′ sends message through BAN 4, BAN 4 simply forwards the data until BAN 3′ contains no information about BAN 3. If any of the information of BAN 3 is captured and sent by BAN 3′, then BAN 4 does not forward it, instead it runs the algorithm to compare the ID and fingerprint of both the BANs (BAN 3 and BAN 3′). In the first level of authentication process, the detection of cloned node occurs in two ways:

a) Local verification
b) Global verification
i) Cloned node detection by neighbor nodes (local verification): path BAN 3 - BAN 4 – BAN 2 – Base station

If node BAN 3 has neighbor BAN 4 which calculates BAN 3′s fingerprint. The message forwarded by BAN 3 has its own fingerprint. Then the neighbor node (witness) which receives the message checks with the fingerprint of BAN 3 stored in it. If it matches, then BAN 3 is considered as normal node. Otherwise, BAN 4 informs base station. Then base station queries BAN 4 which in turn replies with the fingerprint of BAN 3. If fingerprint of BAN 3 stored at the neighbor BAN 4 differs with the BAN 3 sent one, then BAN 3 is revoked as a clone node.

By this, nodes with same fingerprint but with different IDs are detected.

ii) Cloned node detection by base station (global verification): path BAN 3 - BAN 4 – BAN 2 – Base station

Base station maintains fingerprint file indexed with ID. It checks fingerprint in different messages sent in previous period of time t-1, t-2,

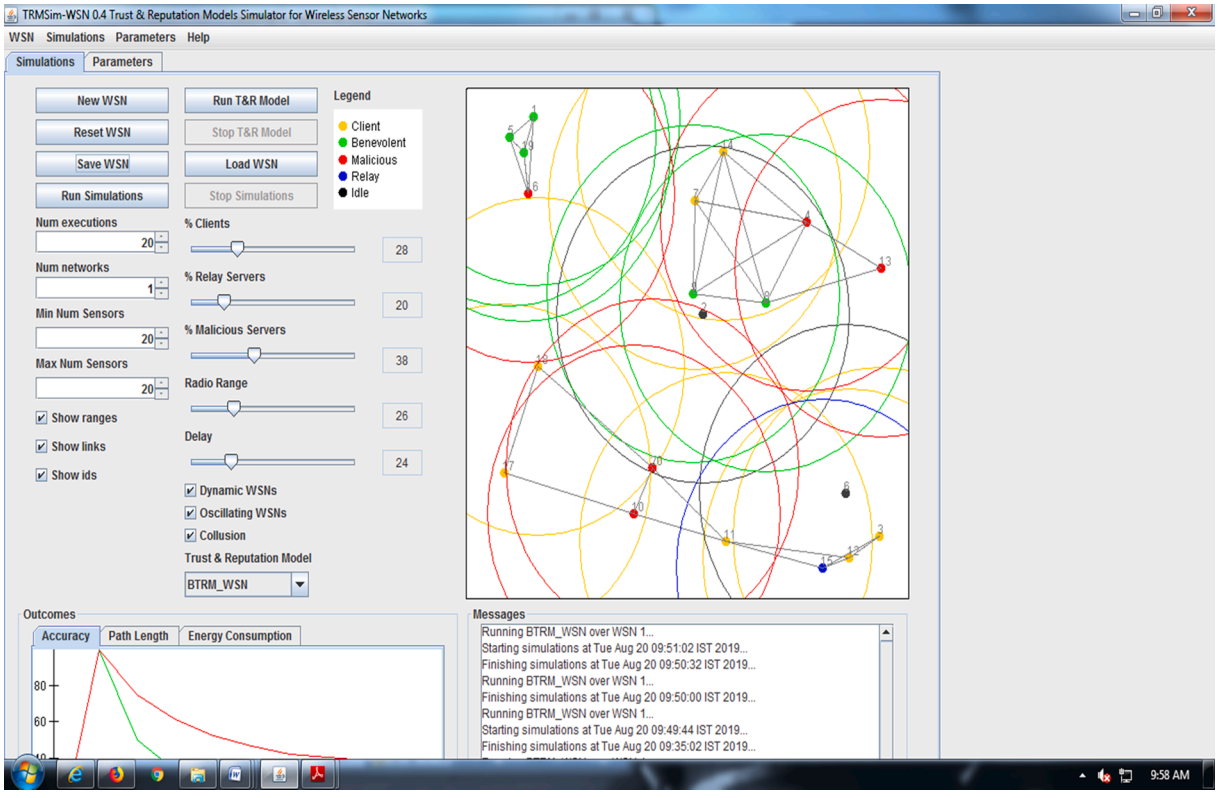

Fig. 5. Network accuracy.

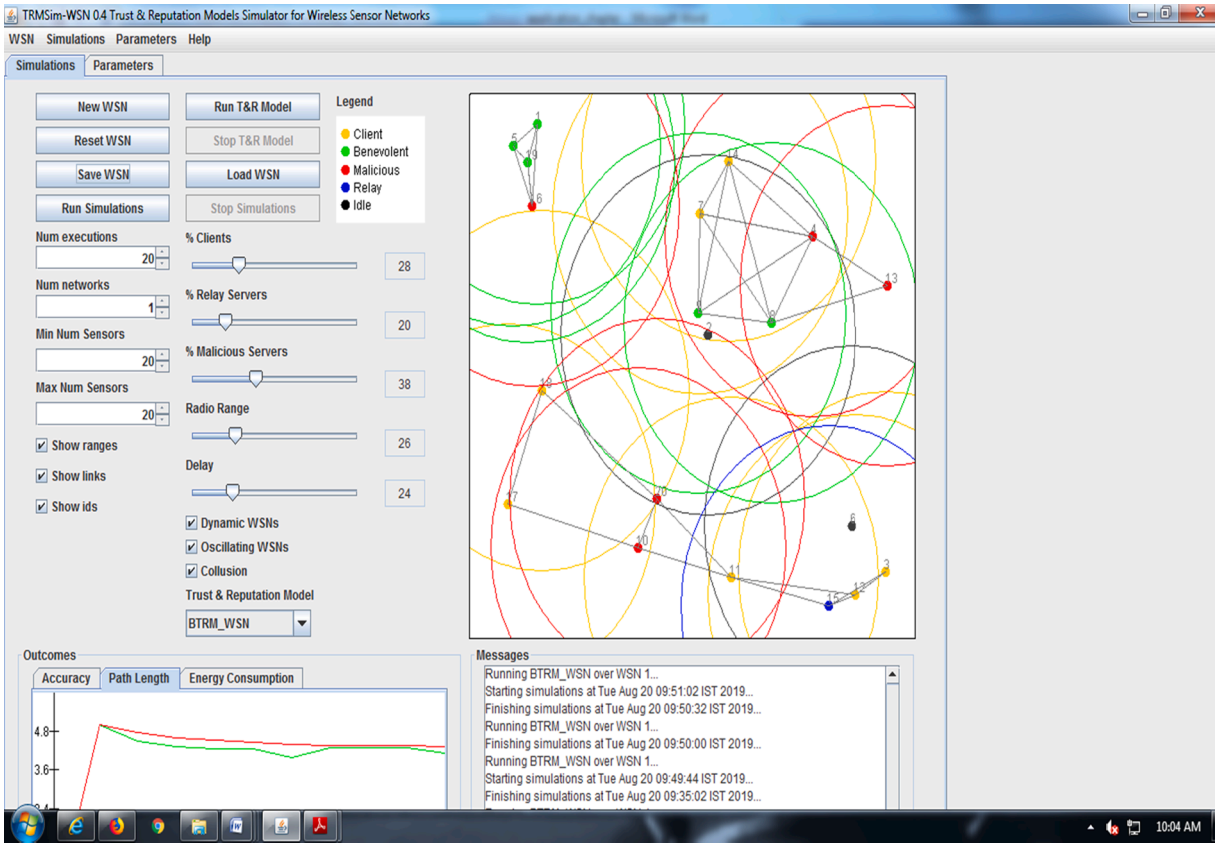

Fig. 6. Path length.

…, t-n by BAN 3. If there are mismatches, base station broadcast revocation message throughout the network to confirm BAN 3 as replica.

By this, node/nodes having with different fingerprints with same ID and different fingerprints with different IDs are detected.

In the second level of authentication process, if BAN 3 is the source, base station is the destination, then BAN 3 - BAN 4 – BAN 2 – Base station path is used in which BAN 3 and base station are not direct neighbours. In this case, BAN 3 is the prover and BAN 4 is the verifier, then BAN 4 is the prover and BAN 2 is the verifier, then BAN 2 is the prover and base station is the verifier, in this way authentication takes place for communication of nodes on the path.

Assuming number of communications between two nodes as two for proving authenticity, communication overhead is 10 bytes (if one value = 1 byte) between two nodes and if number of neighbours is considered as four for all nodes uniformly, then storage overhead is (4*4) 16 bytes for each node. The fingerprint takes no more than 2 bytes to be included in a message even for number of nodes M = 1,00,000.

6. Simulation and experimental results

EMABRD, SACOP and FZKA algorithms are evaluated using simulation and experiments at real-time. The parameters taken for analyses are storage overhead, communication overhead and detection probability. The parameter definitions are:

The number of control packets generated divided by the number of data packets received is the overhead.

- Storage overhead
  Average number of bytes required to store the values in each node
- Communication overhead
  The transmission and reception of total number of packets by the node
- Detection probability
  The number of times the compromised nodes detected successfully divided by the total number of times repeated for detection of compromised nodes

For analyzing the three proposed algorithms, Trust and Reputation Models Simulator (TRMSim) is used. Distributed systems such as peer-to-peer networks, WSNs and Multi-agent systems are simulated using TRM simulator. By adjusting various parameters such as percentage of malicious nodes, communication range, delay etc., this generic tool is used to test and compare the trust and reputation models.

6.1. Simulation analysis using TRM simulator

Within the simulation area, ten nodes are randomly deployed and simulated for 100 rounds. Between the nodes and the home gateway, the transmission range is set to 5 m. The configuration among 10 nodes is 28% are clients, 20% are relay servers, 38% are malicious servers, 26% of radio range, 24% delay. The following simulation shows the results of network accuracy, transmission path and energy consumptions for all executions corresponding to the configured values similar to that used in Anandkumar et al [28]. The considered algorithms are tested in a variety of irregular network topologies. Assuming all the packets reaches the destination node through intermediate hops with minimum packet loss. Even that loss is solved in lower layer protocols by retransmission mechanisms. Simulation result takes average number of iterations as 20.

Simulation results of trust and reputation model is shown in Fig. 5 which indicates deployment of nodes and its range of communication. It also shows the nodes' accuracy and its path of communication between the nodes.

Simulation results of trust and reputation model is shown in Fig. 6 which indicates the path of communication between the nodes in

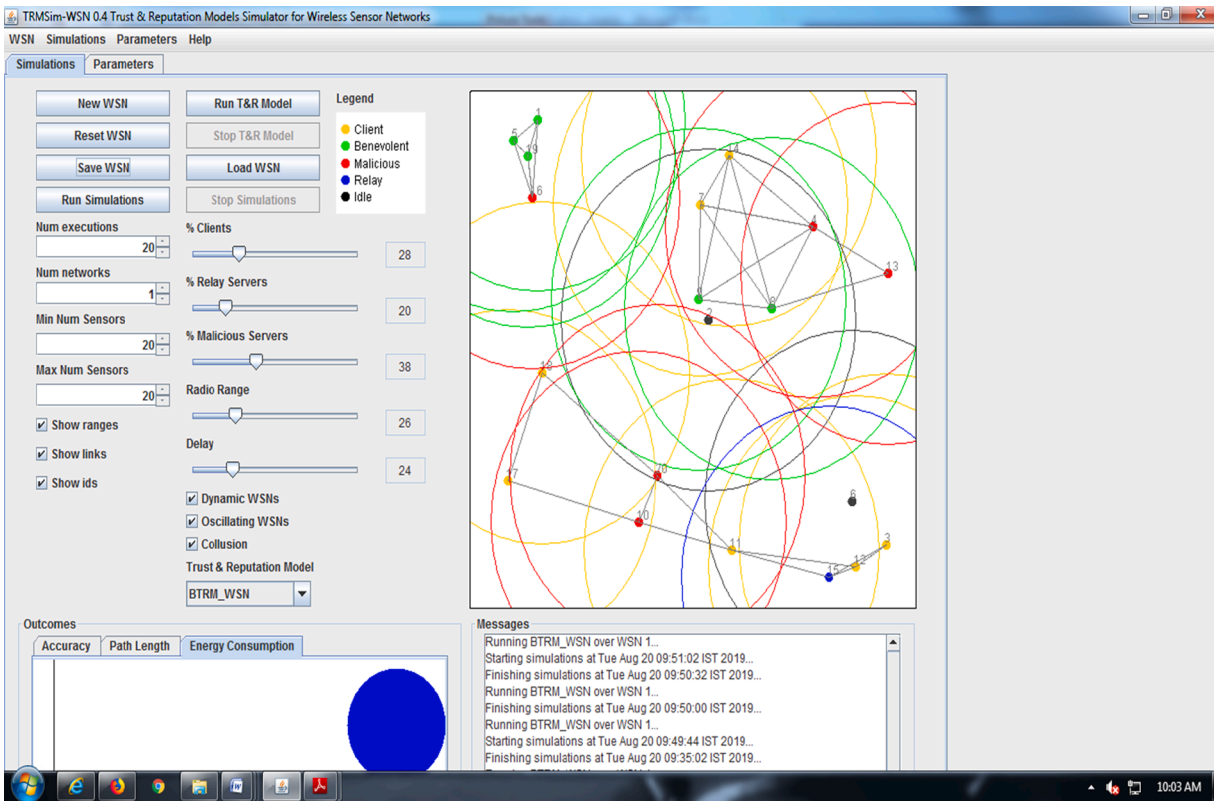

Fig. 7. Energy consumption.

Fig. 8. Six sensor motes with Coordinator at the centre.

current and average scales.

In Fig. 7, simulation results of trust and reputation model is shown that indicates the expenditure of energy by the nodes at the end of execution of all rounds.

6.2. Real-time experiment

The practical implementation of node replication attack in MoteView software is shown in below screenshots.

The arrangement of six medical sensing WSN motes connected to the central coordinator is shown in Fig. 8. In MoteView software, the nodes are arranged in star topology for execution of algorithms.

The motes' communication with the gateway and measurement of corresponding values in periodic time intervals are shown in Figs. 9 and 10.

Due to replication of node, topology change is shown in Fig. 11. The mote with ID 5299 is captured and replicated as mote ID 5325. The replicated mote ID 5325 is now present in two different locations in the network. The original mote ID 5325 communicates directly with the gateway but the replicated mote ID 5325 communicates through mote ID 5315 in multihop manner. The original and replicated motes with ID 5325 communicate with the gateway continuously resulting in reception of messages by the gateway at irregular intervals. But in real-time, the replicated node is distant from the gateway and within the transmission range of any of the node in the network.

When the coordinator encounters conflict location of the node with same ID 5325, the detection algorithm is executed. In FZKA algorithm, unique fingerprint value assigned to each node is used to identify the replicated node with ID 5325 and second level of verification is done at base station.

7. Performance characteristics

The performance of EMABRD, SACOP and FZKA algorithms are analyzed against various parameters viz., storage overhead, memory overhead, detection probability, survival nodes and energy overhead.

7.1. Storage overhead

The behavior of nodes' on different intervals of time period is depicted in Fig. 12. The analysis also indicates that the storage overhead of EMABRD, SACOP and FZKA algorithms increases with increase in iterations. On an average, the number of bytes stored in each node is 35, 142 and 93 in EMABRD, SACOP and FZKA algorithms respectively in all iterations.

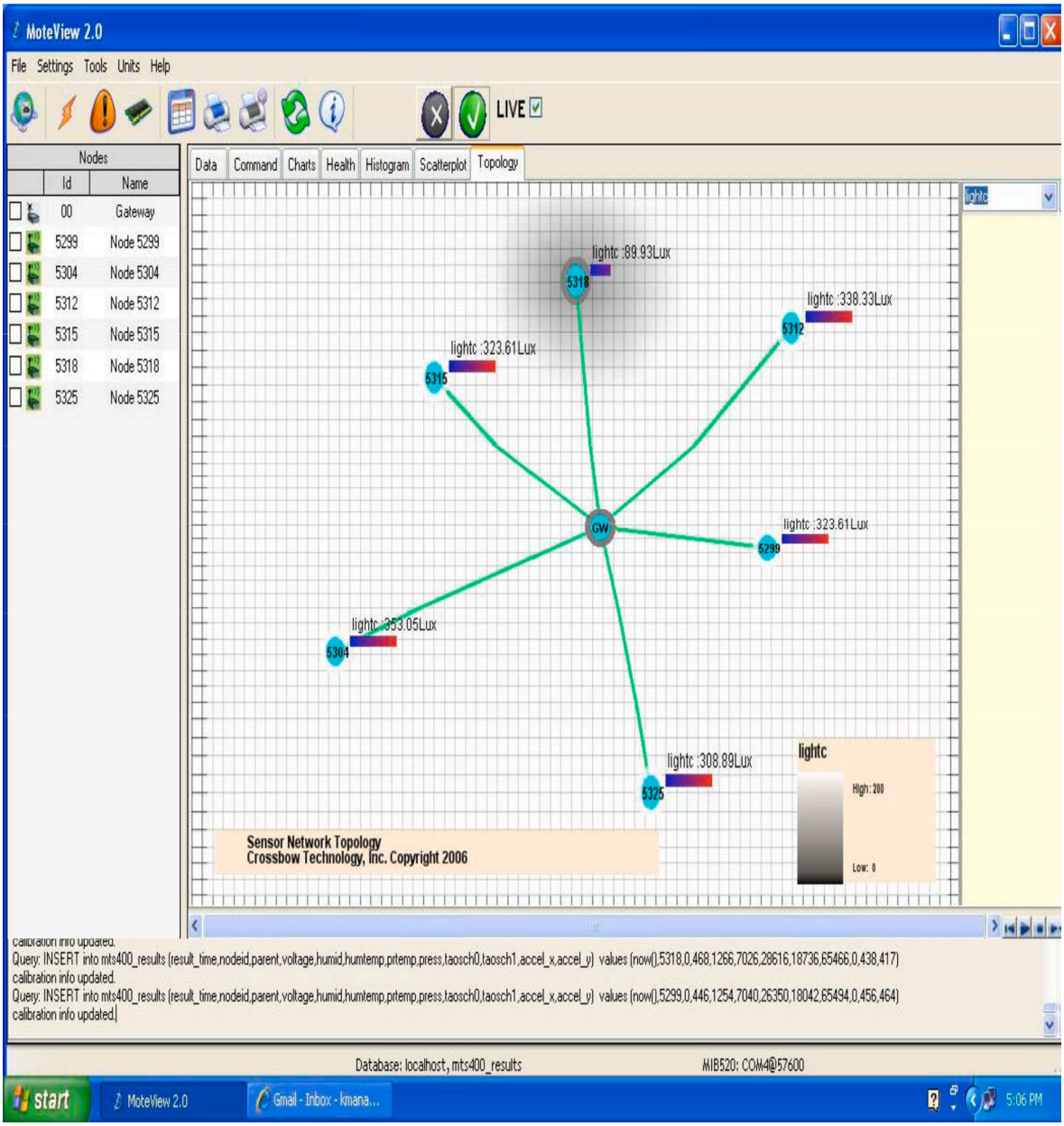

Fig. 9. Six sensor motes communication with Gateway.

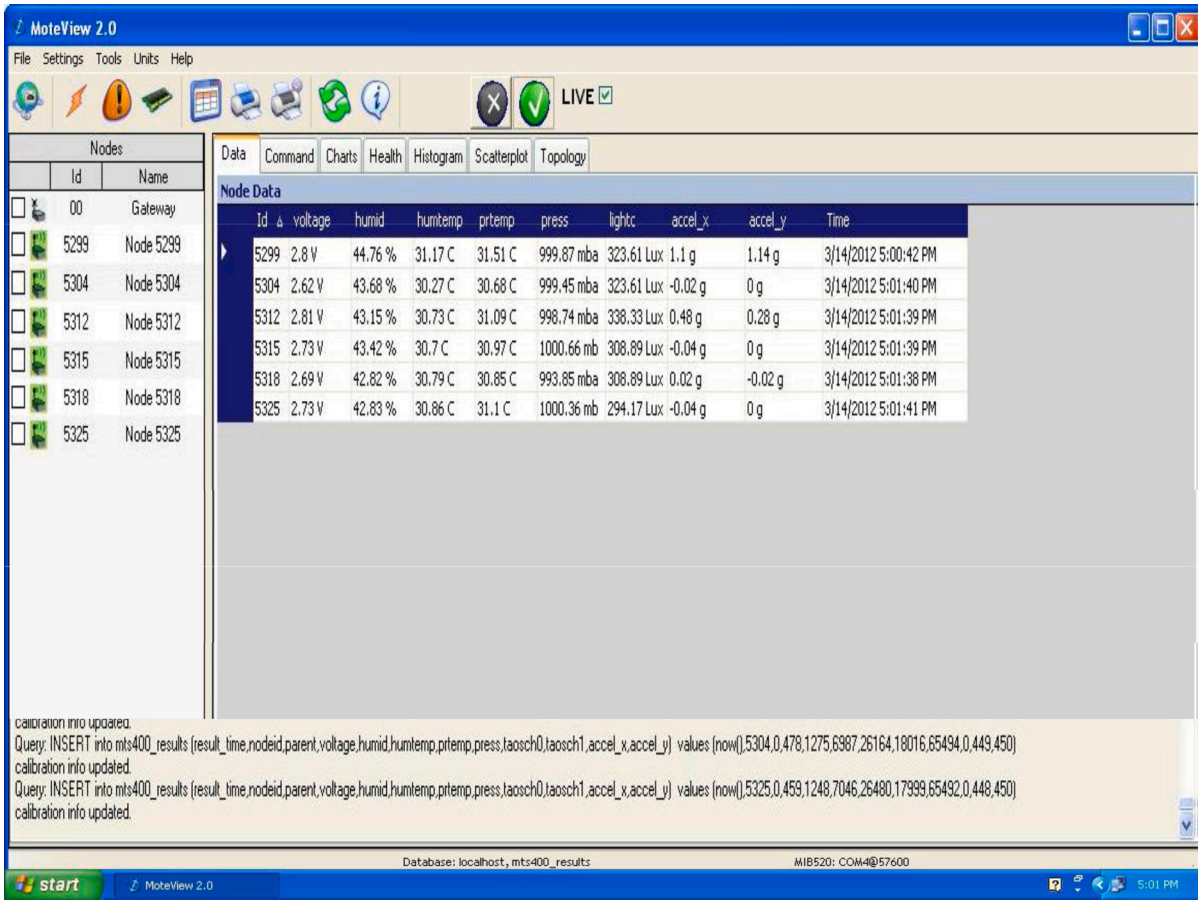

Fig. 10. Sensor motes recording the values.

7.2. Communication overhead

The number of messages transmitted and received directly affects the rate of consumption of energy. Depending on the battery, the operating life of a node depends. Different pattern of node exhaustion occurs due to different energy overheads in three algorithms. Average number of messages transmitted and received per node is shown in Fig. 13 during the replica node detection process in three algorithms. At 20th iteration, the communication overhead is 90 for EMABRD, 150 for FZKA and 180 for SACOP.

7.3. Detection probability

Detection probability at different protocol iterations is shown in Fig. 14. At 5th iteration, the detection probability is 0.85 for EMABRD, 0.9 for FZKA and 0.92 for SACOP. SACOP shows better detection probability compared to EMABRD and FZKA for all considered iterations.

7.4. Survival nodes

Depending on the battery, the operating life of a sensor node lies. The three proposed methods exhibit different survival patterns. When the algorithms execute to detect replica node, energy remaining after each set of iterations is shown in Fig. 15. At 25th iteration, the number of alive nodes is 23 in EMABRD, 64 in FZKA and 56 in SACOP. Among the three proposed methods, the lifetime of the network is high in FZKA compared to SACOP and EMABRD.

7.5. Energy overhead

For the different number of attacker scenario, energy consumption of EMABRD, SACOP and FZKA techniques is shown in Fig. 16. Normally any attack consumes more energy than the normal node. Replica node, in particular, energy consumption gets doubled for every increase in fake identity creation. So, when the number of attacker node increases, energy consumption also increases. Especially in EMABRD, all the nodes transmits the energy information to the sink node periodically in the presence of replica attack, energy consumption is high compared to other two schemes. In SACOP, clustered network in which reliable path is established based on recommendation from neighborhood nodes. So, energy consumption is considerably reduced compared to EMABRD. In FZKA, clustered network with local and global detection method is used for replica node identification, so energy consumption is considerably reduced compared to SACOP.

8. Conclusion

In the proposed EMABRD algorithm, detection of replica node is based on energy consumption threshold. Replica nodes with multiple fake identities have to spend additional energy than that of normal nodes. In case of periodic events, this method is able to distinguish between replica and normal nodes based on the difference between actual and predicted energy. But when the events arrive randomly, misdetection occurs. So, EMABRD incurs decreased detection probability and storage and communication overheads compared to SACOP and FZKA.

In the proposed SACOP algorithm, the trust value is calculated based on the recommendations from the neighbor nodes incurs storage and

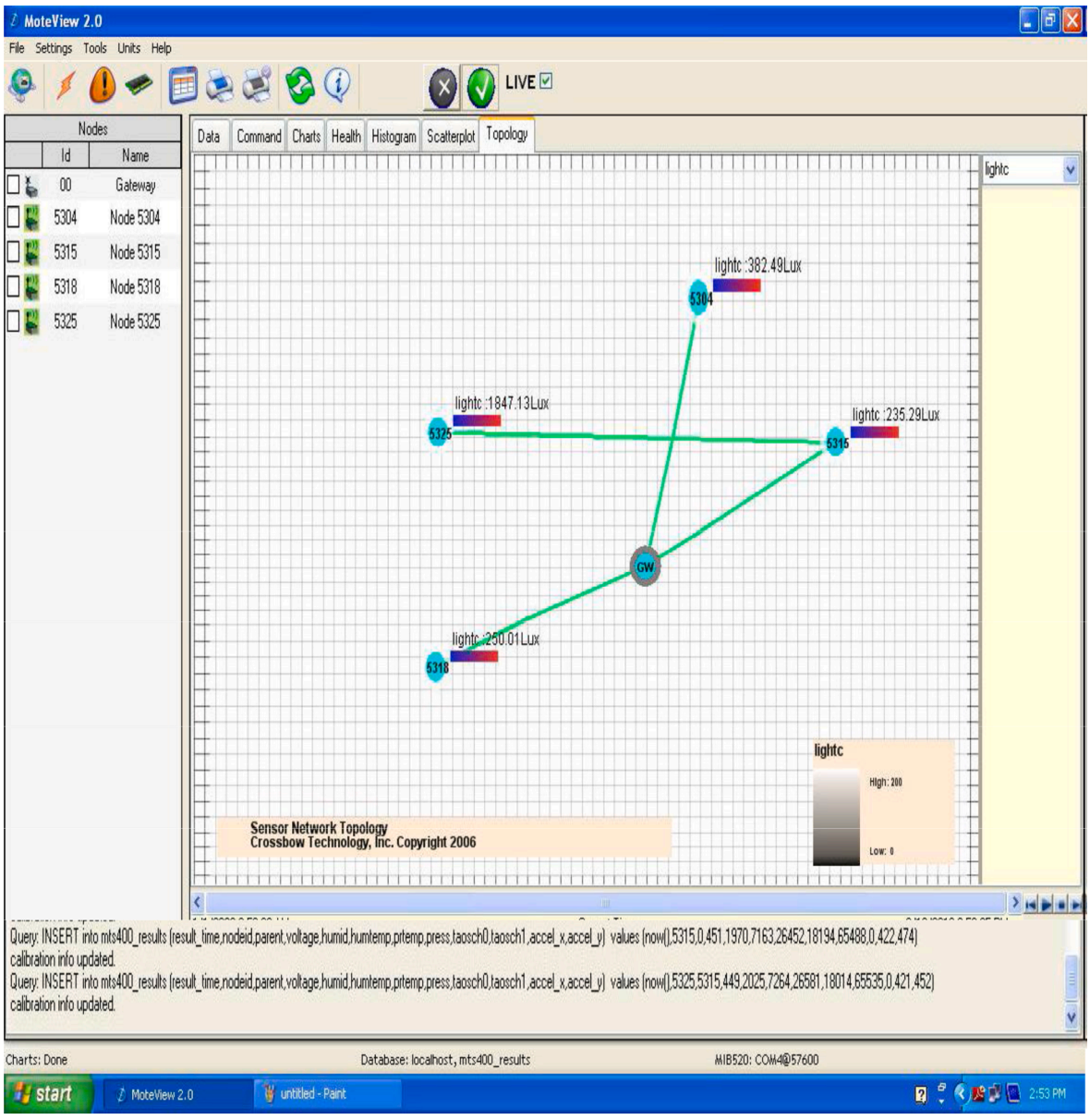

Fig. 11. Change in topology due to node replication.

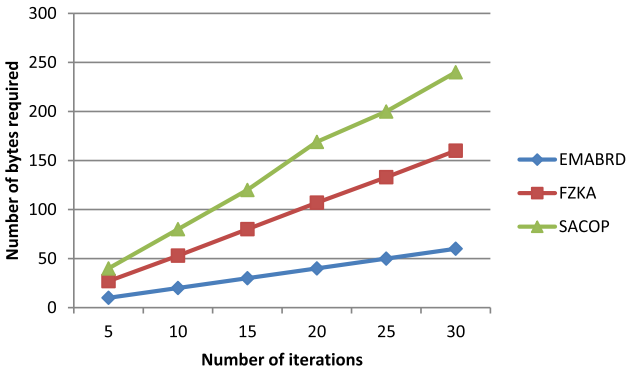

Fig. 12. Storage overhead.

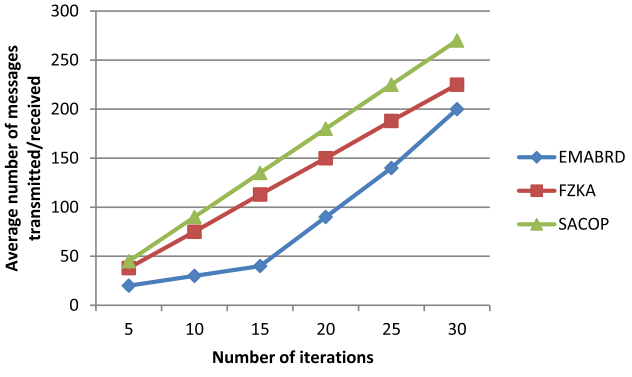

Fig. 13. Communication overhead.

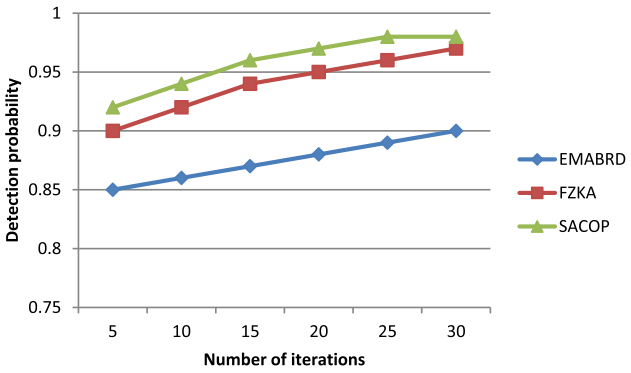

Fig. 14. Detection probability of malicious node.

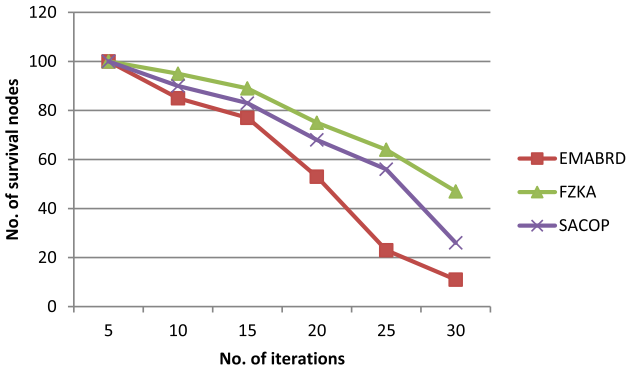

Fig. 15. Number of survival nodes.

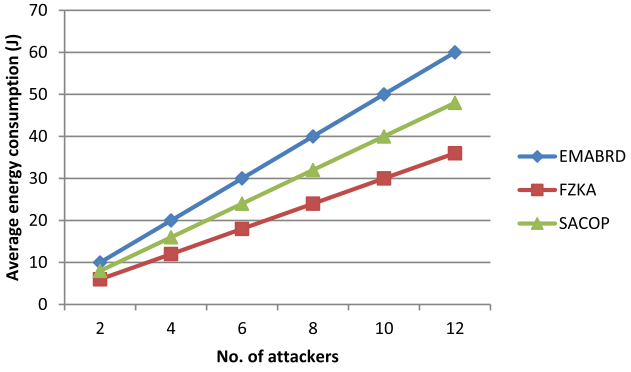

Fig. 16. Average energy consumption in the presence of attackers.

communication overheads. And the trust value is maintained stable in case of any interaction and becomes highly sensitive to attack characteristics using regulator and penalty functions. So, SACOP have higher detection probability and faster detection of malicious nodes at the expense of increased storage and communication overheads compared to EMABRD and FZKA.

In the proposed FZKA algorithm, there is no changing factor based on the network size or workload. So, detection rate increases unlike other existing energy trust systems. Hence, FZKA have higher detection probability compared to EMABRD. Each node stores its own fingerprint and each CH stores the fingerprint of its member nodes. BS stores the fingerprints of only the CH nodes. CHs and BS are only involved in replica detection. So, FZKA have decreased storage and communication overheads compared to SACOP.

CRediT authorship contribution statement

S. Anitha: Writing - review & editing, Conceptualization, Writing - original draft, Formal analysis. **P. Jayanthi:** Software, Writing - review & editing. **V. Chandrasekaran:** Methodology, Writing - review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

The research work was partially funded by University Grants Commission South Eastern Regional Office, Hyderabad under Minor Research Grant with P.No:3620 for the title, “Pattern Improvement in Rank based Association Rule Mining for Energy Conservation in Wireless Sensor Networks”.

References

[1] C. Maxim, B. Zubair, B. Oladayo, Z. Sherali, Internet of things (IoT): research, simulators and testbeds, IEEE Internet Things J. 5 (3) (2018) 1637–1647.
[2] J. Sakhnini, H. Karimipour, A. Dehghananha, R.M. Parizi, G. Srivastava, Security aspects of internet of things aided smart grids: a Bibliometric survey, Internet of Things (2020) 1–45, https://doi.org/10.1016/j.iot.2019.100111.
[3] S. Maheswaran, P.G. Kuppusamy, S.M. Ramesh, T.V.P. Sundararajand, P. Yupapin, Refractive index sensor using dual core photonic crystal fiber – glucose detection applications, Results Phys. 11 (2018) 577–578, https://doi.org/10.1016/j.rinp.2018.09.055.
[4] P. Kakria, N.K. Tripathi, P. Kitipawang, A real- time health monitoring system for remote cardiac patients using smartphone and wearable sensors, Int. J. Telemed. Appl. 2015 (2015) 1–11.
[5] A. Darwish, A.E. Hassanien, Wearable and implantable wireless sensor network, Solut. Healthcare Monit. Sens. 12 (2012) 12375–12376.
[6] M. Shanmugam, S. Nehru, S. Shanmugam, A wearable embedded device for chronic low back patients to track lumbar spine position, Biomed. Res. 2018 Special Issue: Special Section: Computational Life Sciences and Smarter Technological Advancement 2018 (2018) S118–S123.
[7] A. Hande, E. Cem, Wireless sensor networks for healthcare: a survey, Comput. Netw. 54 (2010) 2688–2710.
[8] K. Vasanth, S. Rachuri, Real time monitoring of environmental parameters using IoT, Wireless Pers. Commun. 112 (2020) 785–808.
[9] J. Ko, C. Lu, M.B. Srivastava, J.A. Stankovic, A. Terzis, M. Welsh, Wireless sensor networks for healthcare, Proc. IEEE, Special Issue Sens. Network Appl. (2010) 1946–1960.
[10] X. Le, M. Khalid, R. Sankar, S. Lee, An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare, J. Netw. 6 (3) (2011) 355–364.
[11] P. Kumar, H.J. Lee, Security issues in healthcare applications using wireless medical sensor networks a survey, Sensors 12 (1) (2012) 55–91.
[12] M Aminian, R.N. Hamid, A hospital healthcare monitoring system using wireless sensor networks, J. Health Med. Inform. 4 (2) (2013) 1–6.
[13] Y. Zhang, L. Sun, H. Song, X. Cao, Ubiquitous WSN for healthcare: recent advances and future prospects, IEEE J. Internet Things 1 (2014) 311–318.
[14] G. Uma Gowri, R. Sivakumar, A novel method of inconsistent collision detection to prevent cloning attacks in high security Wireless Body Area Networks, Int. J. Eng. Technol. 6 (2) (2014) 615–626.
[15] V. Mainanwal, M. Gupta, S.K. Upadhayay, A survey on wireless body area network: security technology and its design methodology issue, in: International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015, pp. 1–5.
[16] M. El-hajj, F. Ahmad, C. Maroun, S. Ahmed, A survey of Internet of things (IoT) authentication schemes, Sensors 19 (5) (2019) 1–43.
[17] M. Ghamari, B. Janko, R.S. Sherratt, W. Harwin, R. Piechockic, C. Soltanpur, A survey on wireless body area networks for ehealthcare systems in residential environments, Sensors 16 (831) (2016) 1–33.
[18] M. Shanmugam, A. Ramasamy, Sensor-based turmeric finger growth characteristics monitoring using embedded system under soil, Int. J. Distrib. Sens. Netw. 10 (6) (2014), 476176.
[19] M. Shanmugam, A. Ramasamy, S. Paramasivam, P. Prabhakaran, Monitoring the turmeric finger disease and growth characteristics using sensor based embedded system —A novel method, Circ. Syst. 7 (8) (2016) 1280–1296, https://doi.org/10.4236/cs.2016.78112.
[20] M. Radhakrishnan, Y. Palanichamy, Concealed multidimensional data aggregation in big data wireless sensor networks, in: Proceedings of the 7th ACM IKDD CoDS and 25th COMAD (CoDS COMAD), 2020, pp. 19–27.

[21] M. Sumit, A. Emad, N. Moein, M.T. Hamidreza, M. Tapas, P. Zhibo, D. Jamal, Smart homes for elderly healthcare - recent advances and research challenges, Sensors 17 (11) (2017) 1–32.
[22] M. Sumit, M. Tapas, M. Jamal Deen, Wearable sensors for remote health monitoring, Sensors 17 (130) (2017) 1–45.
[23] M. Numan, F. Subhan, W.Z. Khan, S. Hakak, S. Haider, G.T. Reddy, A. Jolfaei, M. Alazab, A systematic review on clone node detection in static Wireless Sensor Networks, IEEE Access 8 (2020) 65450–65461.
[24] C. Kakali, An improved authentication protocol for wireless Body Sensor Networks applied in Healthcare applications, Wireless Pers. Commun. 111 (2020) 2605–2623.
[25] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, K.S. Kwak, A comprehensive survey of wireless body area networks, J. Med. Syst. 36 (2010) 1065–1094.
[26] S. Anitha, P. Jayanthi, K. Lalitha, V. Chandrasekaran, Secured ant colony optimization based on energy trust system for replica node attack detection, Int. J. Emerg. Technol. 11 (2) (2020) 104–109.
[27] S. Anitha, P. Jayanthi, A two-level authentication scheme for clone node detection in smart cities using internet of things, Comput. Intell. 6 (7) (2020) 1–21.
[28] K.M. Anandkumar, C. Jayakumar, Prevention of clone attacks in pervasive healthcare environments, Eur. J. Sci. Res. 72 (3) (2012) 348–359.
[29] B. Rezaeianjauybari, Y. Shang, Deep learning for prognostics and health management: state of the art, challenges and opportunities, Measurement 163 (2020) 1–29.
[30] R. Janarthanan, S. Doss, S. Baskar, Optimized unsupervised deep learning assited reconstructed coder in the on-nodule wearable sensor for human activity recognition, Measurement 164 (2020) 1–11.