Intelligent mobile agents collaboration for the performance enhancement in wireless sensor networks

A. Vijayalakshmi*
Department of Electronics and Communication Engineering,
Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya University,
Kanchipuram-631561,Tamil Nadu, India

and

Department of Electronics and Communication Engineering,
Sri Manakula Vinayagar Engineering College,
Pondicherry University,
Puducherry 605107, India
Email:vijilakshan@gmail.com
*Corresponding author

T.G. Palanivelu
Department of Electronics and Communication Engineering,
Sri Manakula Vinayagar Engineering College,
Pondicherry University,
Puducherry 605107, India
Email:tgpalanivelu@gmail.com

Abstract: Wireless sensor network consists of energy-dependent environment monitoring sensor nodes with sensing, computing, storing and communicating components with power unit. As the network is open to all other devices, incorporating security becomes a challenging task for the resource-constrained wireless sensor networks. Mobile agent’s deployment provides solution to the problems occurring in WSNs. We define an intelligent mobile agent (IMA)-based security optimisation in which different agents govern the network performance such as routing, security check and transmission. Node’s behaviour, available energy and congestion at the link are analysed for every transmission by different agents that ensure the secure communication by eliminating attackers from the routing path. Different from the other agent-based routing schemes, IMA utilises minimum agents for even a large scalable network. The process is simulated, and the results prove that IMA provides enhanced performance and secure communication.

Keywords: dispatcher agent; hashing; intelligent mobile agent; mobile collector agent; scrutinising agent; trust computation; WSN.


Biographical notes: A. Vijayalakshmi received her B.E. degree in Electronics and Communication Engineering from Madras University during 1998. She got Master’s degree in Electronics and Communication Engineering from Pondicherry University. She is doing research in the area of Wireless Sensor Networks at Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya University, Kanchipuram. She is presently working as an Associate Professor in the Department of Electronics and Communication Engineering at Sri Manakula Vinayagar Engineering College, Puducherry. She has 17 years of teaching experience. She has published eight papers in international journals and presented 15 papers in national and international conferences. Her research interests include wireless communication, network security, collaborative mobile agents and information processing. She is a life member of Indian Society of Technical Education.

T.G. Palanivelu obtained his Bachelor and Master degrees in Electronics and Communication Engineering from College of Engineering, Chennai and Doctoral degree from Indian Institute of Science, Bangalore. He is presently working as Professor in the Department of Electronics and Communication Engineering at Sri Manakula Vinayagar Engineering College, Puducherry. He was a former principal of Pondicherry Engineering College, Puducherry. He has more than 40 years of
1 Introduction

Wireless sensor networks have drawn great attention due to its applications and research issues. The most considered issues include security and energy optimisation, because nodes are built with limited energy. To increase the node lifetime, client server model is considered. In the traditional client server method, the client will be destination node, and server will be source node. The source node on reception of requests from the client collects the data and transmits to the sink node which increases the bandwidth and energy. Mobile agents provide solutions to these issues which act as a middleware that migrates between clients within the network. The mobile agents behave according to the network and provide data to the clients on request. The mobile agents has more benefits such as reduction in communication cost, non-parallel execution, direct management, dynamic placement of software and mitigation of distributed applications. The mobile agents are scalable to collect data and transfer the data. The relocation of mobile agents are classified as:

a. strong migration - the mobile agents that migrate with codes and full execution states
b. weak migration - the mobile agents which migrate carrying the codes have partial execution states.

These mobile agents communicate with other agents within a network as well as mobile agents in other networks too. Because the mobile agents are more prone to attacks, it is mandatory to provide security. In networks, mobile agents have the opportunity of attacks in two ways namely:

a. the host may be considered as malicious
b. the mobile agents may be considered as malicious.

The mobile agents provide solutions for flexible networks, when executed locally it utilises the functions of the node. It also provides solutions for network management, active networking, mobile computing and cloud computing.

The rest of the paper is organised as follows: Section 2 describes Related Works; Section 3 explains the Problem Identification and Definition; Section 4 defines the Proposed Method. Finally, the Results and Discussion are explained in Section 5 followed by Conclusion and future enhancement in Section 6.

2 Related works

Xu et al. (2013) proposed an authentication model which provides authenticity and lower overhead in communication, in comparison with other authentication models in wireless sensor networks. The proposed authentication model secures the network in terms of packet loss, tampering and malicious attacks in sensor networks.

Dagdeviren et al. (2010) have studied various mobile agent technologies and the implementation of mobile agents on wireless sensor networks for applications according to their objective and cost for research issues.

Bai et al. (2009) calculated the energy consumption and its performance in a reliability model by employing mobile agent in wireless sensor networks. A middleware is developed, which tends to reduce data retransmission and bandwidth constraints. The results showed that mobile agent migrates to sink node for each duty cycle. It validates that duty cycle can be achieved with power management schemes for heterogeneous wireless sensor networks.

Hamzi et al. (2013) designed multiagent architecture for wireless sensor networks applications in which agents are autonomous and have the privilege of entering and leaving the network at any instance and solve computational problems smoothly. On comparison with normal mobile agents, MAS can reconfigure according to the network changes which reduces complexity.

Wang et al. (2011) discussed the advancements of organising multiple mobile agents, to improve energy and task duration. The multiple mobile agents in networks are addressed as follows:

a. the number of mobile agents to be used
b. the number of source nodes that are to be assigned for each mobile agent.

A comprehensive study has been made for system architecture, middleware design and hardware design that have been estimated.

Sheela et al. (2012) have proposed a model for security against attacks such as clone and sink hole attacks and agent routing algorithm to provide paths for mobile agents and compared for communication overhead and cost with detection systems without mobile agents.

Jiang et al. (2015) have proposed an efficient distributed trust model (EDTM) algorithm for wireless sensor networks which considers the trust behaviour of nodes and to prevent the security breaches for nodes more effectively. The received packets by the sensor nodes are studied for direct trust, recommendation trust and indirect trust. Simulation results represents that EDTM is efficient and attack resistant trust on comparison with other trust-based models for wireless sensor networks.

Zhou et al. (2015) have proposed some methods for efficient usage of watchdog timers for energy conservation and fusion of algorithms for effective schedule of watchdog timer.
timer tasks according to trust behaviour of sensor nodes and evaluated on WSNET platform.

Rajendiran et al. (2011) proposed an efficient security algorithm known as elliptic curve cryptography. A private key is generated on the basis of point doubling mathematical model. When two nodes share their private key, a link is determined between these two nodes. According to the key size and sharing of private keys with other nodes, the link is established between them. Simulation analyses revealed that this method resists to various brute force attacks, random attacks with minimal resource and better connectivity.

Li et al. (2012) proposed a scalable authentication scheme based on elliptic curve cryptography, i.e. source anonymous message authentication that allows the sensors’ nodes to transmit infinite number of messages without going through threshold problem and provides message confidentiality. The simulation results showed that the proposed method is more efficient in terms of computational overhead, energy efficiency and delivery ratio when compared with existing elliptic curve cryptography.

Usman et al. (2012) proposed middleware architecture for mobile agents in wireless sensor networks’ applications to overcome the drawbacks of habitual client/server architecture models. A middleware is built on the top of an operating system in WSN. It provides on-demand intrusion detection mechanism for middleware.

Yao et al. (2015) have proposed a data aggregation protocol named energy efficient delay aware life time (EDAL) balancing data collection which is a hybrid combination of centralised heuristic and distributed heuristic which overcomes the problem of computational overhead and increases the scalability of the network. The protocol increases lifetime of the nodes without affecting the delay of the packets.

Leu et al. (2015) proposed a clustering protocol for WSN called regional energy aware clustering with isolated nodes (REAC-IN). The cluster heads are selected according to their weights, and the cluster of nodes is chosen according to the residual energy of the nodes. To extend the network lifetime, the average energy of the cluster and distance between sensor and the sink is determined to find either the isolated nodes send it data to cluster head or to the sink.

Hsueh et al. (2015) proposed a cross layer secure scheme integrating MAC Protocol known as two-tier energy efficient secure scheme (TE2S) for security against DoS which reduces the lifetime of the networks. The performance results have shown that the combination of defensive mechanism with check points can defense attacks and efficient in both transmitter and receiver-initiated schemes with less energy throughput performance.

3 Problem identification and definition

In WSN, security using mobile agent has drawn much attention for researchers in the recent years. In the existing methods, routing complexity and transmission overhead are high due to multiple and longer decision-making process. We propose an intelligent mobile agent-based wireless sensor network (IMAWSN) to provide security and employ mobile agents with less computational complexity and overhead. Here, the process is distributed using intelligent mobile agents (IMAs), minimising the early energy drain of sensor nodes when compared with the previous approaches. Besides, a dedicated agent monitors the behaviour of each transmitting node with higher trust factor recommending it as the legitimate neighbour. A node with duplicate entry, larger response time and higher packet drop are discarded from the routing path.

3.1 Sinkhole attack

In a sinkhole attack model, a compromised node attracts traffic from a specific network region by distributing its best routing features through which it enters the routing process and manages to replicate its type. Usually sinkhole attack performs routing entry towards the nodes located near the sink. If the neighbouring nodes adapt with the routing metrics of the compromised node, the traffic originating will end up as those from the same type of successes. Link estimation models and node monitoring kind of prevention systems can able to eliminate such attacks at both early and provocative stages (Krontiris et al., 2007).

3.2 Clone attack

A cloning node gathers the neighbour information and replicates it on to multiple nodes that are to prevent early detection, and the central node redeploy the replicated nodes to different parts of the network. Clone attack results in selective node forwarding, DoS and packet amending attack. Clone attacks are detected using cryptographic solutions and key-based secure transmissions (Zheng et al., 2013).

3.3 Packet delivery factor

Packet delivery ratio Packet delivery factor (PDF)) is the ratio between packet received and packet sent for a higher throughput. Packet delivery factor (PDF) factor must be high, whenever a link failure or interruption occurs, PDF ceases.

3.4 Route error

When a packet encounters a route or link breakage, the transmitting node sends a route error (RERR). Upon receiving a route error, the transmitting node reroutes the packet.

3.5 False acknowledgement

A null acknowledgment that is generated by a malicious node to capture and compromise nodes is called a false acknowledgment.

4 Intelligent mobile agents in wireless sensor networks

Our methodology aimed to provide security against cloning and sink hole attacks using mobile agents. In previous
methods, more number of mobile agents has been utilised, which increases computation overhead, due to maximum energy drain that the mobile agents have been incapable to handle multiple attacks. Each distributed process agent communicates with each other sharing the in range node behaviour and routing process.

The proposed system includes three types of intelligent agents: mobile collector agent, dispatcher and scrutinising agent. Mobile agents will have privileges which have control over network and follow a route in migrating within a network and network in remote. Mobile agents decide itself and authorise timely information which provides stability by reducing computational overhead, energy minimisation and eases bandwidth constraints.

The wireless sensor network architecture with IMA is illustrated in Figure 1.

**Figure 1** IMA in wireless sensor network

![IMA in wireless sensor network](image)

The functions of the agents are illustrated in Figure 2.

**Figure 2** Intelligent mobile agent classification and its function

![Intelligent mobile agent classification and its function](image)

The lifetime of a mobile collector agent is computed after each transmission for its replacement. The lifetime $LT$ of a node is given by (5)

$$LT = \frac{E_{RE}}{H - 1} \times \sum_{i=1}^{H} R_{ij}(t)$$

$H$ - hops

$LT$ - lifetime of a node

$R_{ij}$ - difference between transmission energy of the $K$th packet and $(K+1)$th packet transmission.

### 4.1 Mobile collector agent

The mobile collector agent migrates throughout the network and cooperates with other MCAs mutually. The MCAs achieve path preferences from scrutinising agent and select the next neighbour nodes. It performs functions such as listener and commander. The MCA monitors the network and commands the dispatcher agent on listening to the scrutinising agent. The source requests to the MCA for determining the path. The MCA changes according to their utility, user mapping resources and energy.

The mobile collector agent lifetime is computed using the residual energy formula, and the next mobile collector agent is selected based on higher lifetime and trust value (Li, 2014; Hsueh, 2015; Maleki et al., 2003).

Residual energy ($E_{RE}$) = $I_{EG} - E_U$

1. $I_{EG}$ initial energy
2. $E_U$ energy utilised

$$E_U = E_{Tx} + E_R$$

3. $E_{Tx}$ transmission energy
4. $E_R$ reception energy

where

$$E_{Tx} = D_{Tx} \times E_{UT}$$

5. $D_{Tx}$ data transmission time
6. $E_{UT}$ energy utilised for transmission

$$E_R = D_{Rx} \times E_{UR}$$

7. $D_{Rx}$ data reception time
8. $E_{UR}$ energy utilised for reception

The collector agent preferences

The collector agents are preferred in the order of agents communicating with maximum active transmitting node. MCAs with high residual energy that deliver packets with minimum delay are chosen with respect to energy.

### 4.2 Dispatcher agent

The dispatcher agent considers mobile collector agents and provides privileges to mobile agents that these agents are
zone-dependent or group dependent, i.e. a group of nodes within the range interacts with collectors. The dispatcher agent maintains a set of records, which includes timestamp specifies the time of transmission and reception and analyses the network for their congestion factor that when the congestion is high, then each of the dispatcher load is distributed among the available dispatcher nodes with high energy. When dispatcher nodes are in active states, the zone remains in sleep state which reduces the energy consumption thus increases the availability of dispatcher nodes that improves disconnection of zones from the network. The process of data transmission and delivery to the destination node are governed by the dispatcher agent. If the number of packets is equal or less than queue length then congestion factor will decrease (Devi, et al. 2013).

\[ Q_c = (1-W_f) \times Q_s + U_{Qc} \times W_f \]

\( Q_c \) - queue length
\( W_f \) - transmission weight factor
\( U_{Qc} \) - current queue utilisation

\[ \text{Link utilisation} = \frac{D_s}{L_d} \]  
(6)

where \( D_s \) is data size
\( L_d \) is link delay

\[ \text{No. of packets} = \frac{D_n}{L_{ar}} \]  
(7)

\( D_n \) - data rate
\( L_{ar} \) - link adaption rate.

\[ L_d = LU_T + A_T \]  
(8)

\( LU_T \) - link utilisation time
\( A_T \) - access time

\[ LU_T = T_R + T_c + T_f \]
\( T_R \) - request time
\( T_c \) - reply time
\( T_f \) - transmission time.

4.3 Scrutinising agent

The scrutinising agent governs nodes activity such as transmissions, sequences and susceptibility. The scrutinising agent delivers two records: forwarding record and halting record. The scrutinising agent examines the trust factor based on PDF, link delay, neighbour ID. For a trusted node, the PDF must be high and link delay must be minimum with least route error and nil false acknowledgement. The categorised trusted nodes are monitored for the current and past transmission histories for the above-mentioned parameters. The nodes that are scrutinised are considered as trusted nodes and are allowed to transmit data. The nodes that functions as an intermediate for transmissions are known as halted nodes. These nodes are not privileged for user application transmission. The scrutinising agent supervises node’s behaviour for sequential transmissions between the intermediate nodes. The scrutinising agent computes the trust factor of each eligible transmitting node using (Shen and Li, 2015)

\[ T_{t_{\text{new}}} = \alpha T_{t_{\text{old}}} + (1-\alpha)T_c (\alpha < 0) \]  
(9)

Where \( T_c \) is currently calculated trust value for period \( t \) and \( \alpha \) is weight factor. The node with high transmissions and less power is fixed with larger value \( \alpha \) where \( \alpha = \frac{D}{P} \) in which \( D \) represents the number of packets dropped in a single transmission and \( P \) is packets queued for transmission.

Interaction trust between two neighbour nodes is computed for each and every transmission using (Reddy and Selnic, 2011)

\[ T_{\text{t}_{n,j}} = (n_jTS_{i,j,t}) \]  
(10)

\( T_{\text{t}_{n,j}} \) - trust between node \( i \) and node \( j \)
\( TS_{i,j,t} \) - set of transmission.

The scrutinising agent considers Genus Function utilisation for trusted nodes alone.

4.4 Key-based security through agent

A secure private key is generated by the dispatcher agent and is utilised for communication between the source and the sink using ECC Genus function. The process of key generation and communication is as follows:

4.4.1 Genus calculation

The Genus is computed based on the fitness function of the raising edge and falling edge. A node is said to be in forwarding state in raising edge and halt state in falling edge. The forwarding state of a node depends upon the trust factor computed from the node state information such as sequence number, next node, packet delivery factor and packet drop. A node in halt state is looked upon for last sequence number, drop, RERR and ACK.

4.4.2 Process of hashing

Consider a genus function \( G \), initiated with a temporal routing hash function \( H \). \( G \) and \( H \) are initialised for all transmissions of the active nodes ‘N’ in the network in the region \((X*Y)\). For a transmission, sender initiates hash \( H \) that is dependent upon the availability of the mobile collector agent and validity of genus \( G \). The genus function’s validity is transmission dependent; \( G \) is invalid if there is an interference or congestion. Genus function factor lies between 0 and 1. \( G \) is not 0 for a node that is transmitting in a sequence. Each node generates its own genus function \( G \) and shares the same with SA for verification. A node that does not share or denies sharing of genus function is announced as malicious by the SA.

In elliptic curve cryptography, the users have a pair of keys a public key and a private key where private keys are known only by users and public keys are shared among all
the users. The mathematical operation of ECC is obtained (Mishra and Singh, 2012).

\[ y^2 = x^3 + ax + b \]  

(11)

Both the values ‘a’ and ‘b’ give different elliptical curves, where

\[ 4a^3 + 27b^2 + k = 0 \]  

(12)

\((x, y)\) satisfies above equations and represents a point of infinity on the curve. The public key is obtained by multiplying private key with a random generator ‘g’ in the curve.

### 4.4.3 Concealed data aggregation

Concealed data aggregation (CDA) is used for secure aggregation of data with minimum delay shown in Figure 3. As the aggregator node is prevented from storing any record information, privacy between the source node and sink is ensured.

In CDA, hop-by-hop authentication process is avoided as there is a chance of revealing security information and message through a compromise attack initiator. This improves the confidentiality of transmission. CDA is an end-to-end encrypted data aggregation scheme that allows collection of cipher text following privacy homomorphism (PH). PH supports collection of encrypted data aggregation and energy efficient secure data aggregation solution to WSNs. CDA integrated with asymmetric PH support ECC with reduced key size that is appreciable for real-time applications.

### 4.4.4 Data authentication

Authentication is carried out using ECC-based signature. Signature generation is described in the following steps (Li, 2014; Mishra and Singh, 2012).

1. Generate a random integer I as follows:
   \[ I = x[N] \]
   - \( x \) - random point on ECC curve
   - \( N \) - maximum possible value on the curve

2. Calculate \( h_p \) - hash packets
   \( m \) - message
   \( r \) - exponentiation
   where, \( r = g^k \mod p \)
   \( g^k \) - random generator
   \( |p| \) - largest prime between the elliptical curve points

3. Calculate sign \( s = rd_h + I[N] \)
   \( d_h \) - random integer of the sender

On using the sign \( s \), each packet is authenticated. Each authenticated packet \( A_{ph} \in \{A_{p1}, A_{p2}, \ldots A_{pn}\} \)

### 4.4.5 Decryption

Decryption is carried out using the below key:

\[ Dm + K * P_r - n_S(k * G) = Dm + k(n_s * G) - n_S(k * G) = Dm \]  

(13)

- \( Dm \) - original transmitted data
- \( N_S \) - sender private key
- \( N_D \) - destination private key
- \( P_D \) - destination public key
- \( R \) - random key generator

### 4.4.6 Data integrity

Data Integrity ensures accuracy, consistency and completeness of the transmitted data at the receiver end. Integrity is checked using the hash-authenticated packets with those received at the destination using the secret key (Xu, 2013; Li, 2014; Mishra and Singh, 2012).

Sender generates a key compromising \((P_i, S_i)\) receiver knows \(P_i\)

The sender creates authenticated packets using Hash function

\[ A_{pi} \rightarrow A_{pm} \Rightarrow A_{pi} \in \{A_{p1}, A_{p2}, \ldots A_{pn}\} \]

\( A_{pi} \) - authenticated packets

1. The receiver receives the data and verifies the received \( R_{pi} \) to \( R_{pm} \) where \( A_{pi} \) is same as \( R_{pi} \) to \( R_{pm} \) received packets based on \( P_i \)
2. Receiver verifies this using the secret key and hash value of \( R_{pi} \)

It accepts packets if

\[ A_{pi} \in \{A_{p1}, A_{p2}, \ldots A_{pn}\} \leftrightarrow R_{pi} \in \{R_{p1}, R_{p2}, \ldots R_{pn}\} \]

### 4.4.7 Data confidentiality

Secret key \( S_{ids} \) known only to the sender and receiver based on their share Pre-IDs. A packet transmitted with the destination node ID is alone provided with secret key \( S_i \) and this ensures confidentiality.

Secret key of the sender \((S_{K(S)})\)

\[ S_{K(S)} = n_s * P_R \]  

(14)

- \( n_s \) - sender private key
- \( P_R \) - public key of the receiver

Secret key of the receiver \((S_{K(R)})\)

\[ S_{K(R)} = n_r * P_S \]  

(15)

- \( n_r \) - receiver private key
- \( P_S \) - public key of sender
5 Simulation results

NS2 simulation has been adopted in this paper to evaluate the performance of the proposed IMA, and the simulation set-up is as given in Table 1.

Table 1  Simulation parameters

<table>
<thead>
<tr>
<th>Simulation and network parameters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Network area</td>
<td>$1000 \times 1000$</td>
</tr>
<tr>
<td>Protocol</td>
<td>DSR</td>
</tr>
<tr>
<td>No. of sensor nodes</td>
<td>100</td>
</tr>
<tr>
<td>Network topology</td>
<td>Flat grid</td>
</tr>
<tr>
<td>IEEE standard</td>
<td>802.11</td>
</tr>
<tr>
<td>Broadcasting range</td>
<td>550 mts</td>
</tr>
<tr>
<td>Application type</td>
<td>CBR</td>
</tr>
<tr>
<td>Application rate</td>
<td>1.0 Mb</td>
</tr>
<tr>
<td>No. of packets</td>
<td>1500</td>
</tr>
<tr>
<td>Simulation time</td>
<td>10 s</td>
</tr>
<tr>
<td>No of mobile agents</td>
<td>8</td>
</tr>
<tr>
<td>Initial energy</td>
<td>10 J</td>
</tr>
</tbody>
</table>

5.1 Comparison with MACAD

5.1.1 Throughput

Throughput is defined as the data transferred in unit time. Figure 4 illustrates the throughput comparison between IMA-deployed WSN network and MACAD-implemented network, where at time 10 s, the observed throughput for MACAD is 1 Mb (approx), the same for IMA-deployed network is 1.8 Mb (approx), levitating the throughput by 55.5%.

5.1.2 Delay

As the number of transmission increases, the number of packets increases, which eventually increases the delay. Figure 5 shows as when compared with MACAD-deployed network, IMA-deployed network shows a minimum delay irrespective of higher transmission. In an IMA-deployed network decision-making process is less, reducing transmission overhead which minimises end-to-end delay in these networks. The observed delay for a set of 100 transmissions is nearly 1 ms for MACAD, whereas for IMA, it is nearly 0.2 ms only.

5.1.3 Energy

The total amount of energy that the network has spent for transmission, decision-making and routing is shown in Figure 6 compared the utilised energy for IMA- and MACAD-deployed networks. As there are maximum transmissions and decision-making, each node spends a little more amount of energy in MACAD whereas the process of IMA is on-demand that minimises the energy consumption of growing network size. Approximately 11.43% of energy is saved for a network size of 40 nodes under IMA.
5.1.4 Misdetection probability
As the false probe increases, misdetection of a node increases. In both IMA and MACAD scenario, misdetection rate increases. When compared with MACAD, IMA has higher detection rate. Figure 7 illustrates that for the detection observed for 0.6 factor of false alarm, detection probability is 0.011 for IMA and 0.0124 for MACAD, decreasing the misdetection by a factor of 0.014.

5.1.5 Disconnection ratio
The probability of eliminating a link due to its adversary effects among the available active links is called disconnection ratio. Figure 8 shows that as the number of nodes increases, the number of links increases eventually increasing the disconnection ratio. The disconnection observed for 30 nodes in an IMA-deployed network and MACAD-deployed network are 43.5 and 46.2%, respectively; the proposed IMA decreases the disconnection ratio by 2.7% when compared with MACAD.

5.1.6 Packet loss
Packet loss refers to the drop that occurs in a transmission between source and destination. As the number of keys increases, vulnerability decreases minimising the packet drop. As IMAs are decision-making systems that work on-demand and the agents are independent, the packet loss is less due to frequent monitoring and change in dispatchers. From Figure 9, the packet loss percent for MACAD for 50 keys is 8.4%, whereas for the same number of keys, only 8% of packet loss is observed in IMA. Therefore, IMA is said to minimise packet loss by 0.4%.
5.1.7 Security level

The exposure to vulnerability and packet loss determines the security level of a network. Figure 10 shows as the number of keys increases, the security of a network increases. As IMAs are smart decision-making agent nodes, they improve the security by instantaneous detection and elimination of threat, which hikes the security level of a network. For 50 keys, the security level observed for IMA-deployed networks and MACAD networks are 8.5 and 3.9%, respectively, improving the security level by 4.6%. The security level is observed only for the key-providing process and not for the scrutinising and rerouting process.
5.2 Comparison with MASAD

5.2.1 Throughput

Throughput is defined as the data transferred in unit time. Figure 11 illustrates the throughput comparison between IMA-deployed network and MASAD-formulated network, where at time 10 s time, the observed throughput for MASAD is 1.09 Mb (approx), the same for IMA-deployed network is 1.8 Mb (approx), levitating the throughput by 35.5%.

5.2.2 Delay

As the number of transmission increases, the number of packets increases, which eventually increase the delay. When compared with MASAD-deployed network, IMA-deployed network shows minimum delay despite higher transmissions. As the number of iterating decision-making process is less and distributed in IMA, it reduces the delay. Figure 12 shows the observed delay for a set of 100 transmissions is nearly 1ms for MASAD, whereas for IMA, it is nearly 0.2 ms only.

5.2.3 Energy

The total amount of energy that the network has spent for transmission, decision-making and routing shown in Figure 13 compared the utilised energy for IMA- and MASAD-deployed network. As there are maximum transmissions and decision-making, each node spends a little more amount of energy in MASAD whereas the process of IMA is on-demand that minimises the energy consumption of growing network size. Approximately 11% of energy is saved for a network size of 40 nodes under IMA.

5.2.4 Misdetection probability

As the false probe increases, misdetection of a node increases. In both IMA and MASAD scenario, misdetection rate increases. When compared with MASAD, IMA has higher detection ratio. For the detection observed for 0.6 factor of false alarm as shown in Figure 14, detection probability is 0.011 for IMA and 0.018 for MASAD, decreasing the misdetection by a factor of 0.7.

5.2.5 Disconnection ratio

The probability of eliminating a link due to its adversary effects among the available active links is called disconnection ratio. As the number of nodes increases, the number of links increases eventually increasing the disconnection ratio. Figure 15 shows disconnection observed for 30 nodes in an IMA-deployed network and MASAD-deployed network are 43.5 and 46%, respectively, the proposed IMA decreases the disconnection ratio by 2.5% when compared with MASAD.

5.2.6 Packet loss

Packet loss refers to the drop that occurs in a transmission between source and destination. As the number of keys increases, vulnerability decreases, minimising the packet drop. As IMAs are decision-making systems that work on-demand and the agents are independent, the packet loss is less due to frequent monitoring and change in dispatchers. From Figure 16, the packet loss percent for MASAD for 50 keys is 8.35%, whereas for the same number of keys, only 8% of packet loss is observed in IMA. Therefore, IMA is said to minimise packet loss by 0.35%.

5.2.7 Security level

The exposure to vulnerability and packet loss determines the security level of a network. As the number of keys increases, security of the network increases. As IMAs are smart decision-making agent nodes, they improve the security by instantaneous detection and elimination of threat, which hike the security level of a network. Figure 17 shows for 50 keys, the security level observed for IMA-deployed networks and MASAD networks are 8.5 and 4% respectively, improving the security level by 4.5%. The security level is observed only for the key providing process and not for the scrutinising and rerouting process.
6 Conclusion

The IMA utilises different nodes for monitoring behaviour and collective data transmission ensuring secure transmission and preventing earlier node energy drain which leverages the network performance far better than the other agent-based systems such as MACAD and MASAD. The overall performance has been analysed for the WSN which proves that IMA is better than MACAD and MASAD in minimising the energy consumption, packet loss, delay and improving other network parameters such as throughput and security level.

References


