International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I11P226

Volume 70 Issue 11, 240-248, November 2022

Original Article

Secure Data Collection in Clustered Wireless Sensor Networks using Fuzzy based scheme to detect Malicious Data Collector

Y. Akshatha[1], A. S. Poornima[2], M. B. Nirmala[3]

[1, 2, 3] *Department of Computer Science and Engineering, Siddaganga Institute of Technology, Karnataka, INDIA.*

[1]*Corresponding Author: akshathay@sit.ac.in*

Received: 18 August 2022 Revised: 09 November 2022 Accepted: 17 November 2022 Published: 26 November 2022

Abstract *- Energy efficiency in a resource-constrained network like Wireless Sensor Network is one of the essential goals to be met for the successful adaptability of any new scheme proposed. Secure Data collection is one of the critical tasks in the wireless sensor network. This paper addresses a novel energy-efficient scheme for secure data collection in the clustered wireless sensor network. The proposed scheme ensures the confidentiality of the data from the point it is sensed until it reaches the central point, that is Base station. Also, the scheme offers a lightweight authentication method to detect malicious data collectors. The proposed authentication scheme first classifies the node using Fuzzy logic. If a classification is inconclusive, it invokes second-level authentication using ECC public key cryptosystem. The experimental results show that around 50% of the time, during multiple MDC visits, it is possible to complete the authentication without using second-level authentication, which involves computing intense cryptographic algorithms. Also, the time complexity experiments reveal that ECC-based authentication is efficient in terms of involved computations.*

Keywords *- Authentication, Mobile data Collector, Fuzzy rule, Malicious Node, Clustered WSN.*

1. Introduction

Wireless Sensor Networks (WSN) is composed of sensor nodes which can sense, process and transmit data to the central node called Base Station (BS). Sensor nodes are resource-constrained with limited computation, storage and communication capabilities and are battery driven. As the participating devices in WSN are sensor nodes, it is very important to conserve energy. This energy conservation leads to the longevity of the participating nodes, thereby increasing the overall network lifetime. Therefore, the schemes/protocols/algorithms proposed for various WSN operations for any category of applications will always look forward to energy efficiency. WSN has many applications [1], such as area monitoring, military surveillance, health care and industrial applications. The range of applications of WSNs now extends to home automation and other areas of human activity [2]. These networks can be distributed or clustered. In distributed WSN, each node participates in forwarding the data to BS. Whereas in clustered WSN nodes organized into small groups called clusters, one node among the group becomes the Cluster Head (CH). The CH is responsible for collecting the data from other nodes in the group and forwarding the same towards the base station. Many pieces of literature [3-8] have proved that the clustering-based approach is efficient compared to distributed approach to network lifetime.

To further improve network lifetime, aggregation /in-network processing [9, 10] is also used. Another way to improve network lifetime is using a mobile node called Mobile Data Collector (MDC) for data collection. Mobile nodes move in a predefined path all over a network to collect data from sensor nodes or cluster heads [11-17]. When mobile nodes are used for data collection, other nodes in the network will save their energy as they are not participating in data forwarding. In this type of network where MDC is used for data collection, it is also important to address the path that has to be taken by MDC in order to cover the network during data collection. Mobility patterns for mobile data collectors are discussed in [34].

Most WSN applications demand secure data collection, thereby restricting attackers/malicious users from accessing data unauthorized. Many schemes [19-21] are proposed for secure data collection using mobile nodes and identifying malicious mobile data collectors. In secure data collection using MDC, we have two important points which require attention when it comes to achieving security. First, achieving confidentiality of the sensed data until it reaches the BS. The second important thing is the detection of Malicious MDC. Always security comes with a cost. In a resource-constrained network like WSN, we always look towards lightweight schemes to optimize energy efficiency. Here lightweight

refers to the schemes which incur less load on nodes concerning computation and communication. Fuzzy logic-based methods have been proven simple and lightweight in computation and communication compared to complex cryptographic algorithms [22-24]. An efficient data-gathering approach using fuzzy logic is proposed in [22]. Here fuzzy logic is used for selecting the optimal route to be followed while gathering data in a WSN to optimize the overall energy. In [23], a fuzzy-based trust model is proposed and evaluated to identify malicious nodes in clustering. The scheme proposed in [24] identifies misbehaving nodes before they actually participate in data transmission.

This paper proposes a scheme for secure data collection using Mobile Data Collector in clustered WSN. The scheme addresses two issues. The first is achieving confidentiality of the collected data, and the second is identifying malicious MDC. Both issues are addressed in an energy-efficient way. To achieve confidentiality of the data, suitable symmetric block cipher algorithms as in [25, 26] and public key cryptosystems [27] are used. To identify malicious MDC, we use a two-level scheme. First, we classify MDC as Malicious (M) or Non-Malicious (NM) based on the proposed Fuzzy mechanism. If the fuzzy mechanism fails to identify MDC as malicious or non-malicious, we invoke the second level authentication, where we use a lightweight public key cryptosystem ECC algorithm [27] to verify the authenticity of MDC. The motivation for this two-level scheme is in WSN; we deal with resource-constrained devices where using cryptographic algorithms every time for authentication becomes costly in terms of computation.

This proposed two-level scheme reduces the heavy computation burden by using a cryptographic algorithm for identifying malicious nodes only when a fuzzy-based mechanism fails to classify the MDC correctly. Experimental results of the proposed scheme show that around 50% of the time, during multiple MDC visits, only the fuzzy method is sufficient to complete the authentication. Other 50% of the time, as the fuzzy method fails to identify a node correctly as a non-malicious node, we will be invoking a second level ECC-based public key cryptosystem on completing the MDC authentication. We also conducted experiments to show that the ECC-based second-level authentication scheme is lightweight in terms of computation overhead incurred on the Cluster head and MDC during this authentication process. Therefore, by restricting compute intense cryptographic algorithms, we can improve overall network lifetime significantly.

In the literature, we find different proposals addressing the use of Mobile data collectors to collect the sensed data in wireless sensor networks. In [28], a survey of such schemes is presented. In this survey, the authors have covered different data collection categories and compared each category in detail concerning different parameters. In work presented in [35], a detailed survey on the use of mobile data collectors for data collection in WSN is discussed. The authors have classified the survey into two significant groups: data collection using mobile sinks and data collection using mobile relay nodes. In each group few necessary protocols are discussed and compared with each other. In the paper, they have also discussed open challenges for data collection using mobile data collectors. Another set of mechanisms/schemes for efficient data collection in WSN is presented in [17]. The authors have discussed all the schemes in brief. To achieve security, authors in [30] have proposed schemes to propagate the information by dividing it into shares. They have proposed four different propagation schemes for information delivery.

Also, the results show that the schemes can secure the transmitted information. Compressive sensing (CS) based data collection schemes can effectively reduce the transmission cost of wireless sensor networks (WSNs) by exploring the sparsity of compressible signals. This work is elaborated in [31]. In [19], three different protocols for secure data collection based on different assumptions and constraints are presented. Here the network model considered is a clustered WSN with a mobile data collector traversing within the network to collect the data from the cluster head. The proposed protocols can identify malicious MDC and maintain the collected data's confidentiality.

2. Proposed Method

This section presents the details of the fuzzy-based scheme proposed for secure data collection. Firstly, we explain the network structure considered in the scheme. The next part elaborates on achieving the confidentiality of the collected data. How data is secured from eavesdropping attacks from the time it is collected from the sensor nodes till it reaches Base Station. The third section summarizes the two-level authentication scheme for identifying malicious MDC. Also, data transfer from MDC to BS is presented. Finally, we will discuss updating the fuzzy variables for the following round of data collection by MDC.

2.1. Network Structure

The network consists of n number of sensor nodes denoted as Si where i ranges from i = 1, ...n, which are used for sensing a particular data type. These sensor nodes are organized into groups called clusters; in a deployed network, let us assume that we have m such clusters. One node within the cluster is selected as Cluster Head CH_i Where j = 1, ...m. Role of the cluster head is uniformly rotated among the nodes in the cluster. Cluster head selection and rotation are made, as explained in [32]. After deployment, cluster formation and the use of secret keys for secure communication within the cluster are explained in [19].

Every sensor node Si forwards the sensed data to the cluster head. The data transfer from CH to BS is done using

Mobile Data Collector (MDC). The MDC considered here is a special node with higher memory and processing capability, which can move in the monitoring area. MDC is deployed by BS to collect the data at regular intervals. This MDC traverse the monitoring area to collect the data, which is carried to BS for further processing. Whenever an MDC visits CH_i The cluster head initiates an authentication process to check whether the MDC is Malicious. Once the authenticity of MDC is verified, CH_i transfers the data to MDC, which is carried to BS.

2.2. Achieving Confidentiality of the Collected Data

For any secure communication, we need shared secret keys. We need appropriate secret keys for confidentiality and two-level authentication in this scheme. Let us discuss in detail the various keys used in the proposed scheme and their purpose and use. Firstly we need a shared secret key between sensor node Si and its respective cluster head CH_i to ensure confidential communication between the node Si and cluster headCH_i. This shared secret key is denoted as k_i. We follow the key distribution scheme as in [19] for sharing this secret key. Sensed data is encrypted by node Si before forwarding it to the respective cluster head CH_i using a symmetric key encryption algorithm [25] with the secret keyk_i. Confidentiality between cluster head and base station BS is achieved using a public key cryptosystem [26], [27]. Each cluster head creates its public and private key pair, denoted asPU_{CH_i},PR_{CH_i} Similarly, respective public and private keys of the base station (BS) are denoted asPU_{BS_i}, PR_{BS_i}. Collected data at CH_i is encrypted usingPU_{BS_i}, only BS can decrypt the data ensuring data confidentiality between CH_i and BS.

Table 1. Notations used in the Proposed Scheme

NOTATIONS	
k_i	The secret key shared between the sensor node and the respective cluster head
M	Sensed data to be transmitted to BS
S_i	i^{th} Sensor Node
CH_i	i^{th} Cluster Head
BS	Base Station
PU_{CH_i}, PR_{CH_i}	Public and Private keys of Cluster Head
PU_{BS}, PR_{BS}	Public and Private keys of Base Station
PU_{MDC}, PR_{MDC}	Public and Private keys of Mobile Data Collector
N_{once}	Random Number
$\{X\}_{k_i}$	Encryption of message X using the secret key k_i

2.3. Two-level Authentication to Identify Malicious MDC

Identifying malicious MDC is essential for secure data collection applications. Traditional public key-based authentication scheme consumes a large amount of memory, computational power, and bandwidth by reducing the computational speed; hence it is expensive for a resource-constrained network like WSN. Therefore, we use fuzzy logic in this proposed work to identify malicious nodes. First, we apply the Fuzzy method wherein the derived fuzzy rules enable us to classify a node as Malicious or Non-malicious, sometimes with the set rules and the current values of fuzzy variables carried by MDC, it is not possible to classify a node as either malicious or non-malicious. If the fuzzy method results are inconclusive, we go for second-level authentication using ECC-based public key authentication [26, 27].

2.3.1. Fuzzy Method

The fuzzy method is considered a practical approach to decision-making. Generally, in fuzzy-based decision-making, we consider a set of fuzzy variables m and the set of decisions n we want to make using these fuzzy variables. Once the fuzzy variables and the required decisions are decided, we will derive a fuzzy rule R which is a mXn matrix. Whenever a decision has to be taken, we will use a factor vector r which forms the current values of fuzzy variables. Then by applying min-max composition, we will obtain an evaluation vector e. With the help of the obtained evaluation vector, the required decisions are taken. This is a general procedure. Now let us see how we are going to use this general method for our problem of classifying an MDC. The following are the fuzzy variables considered in this scheme:

1) Trust Value (TV): The base station assigns initial trust. Whenever MDC visits CH, during authentication between CH and MDC, if second-level authentication using the public key system is processed, it is notified to BS, and BS will recalculate the trust value. Trust value will increase if CH and MDC authentication is successful by using only the fuzzy method. Otherwise, trust value will decrease if second-level authentications are used for authenticating MDC.
2) Visit Interval (VI): For the entire deployment area approximate interval at which MDC will visit the CH is studied and the time interval considering the delay parameters is calculated initially, and the same is used as a parameter for fuzzy-based authentication.
3) Past Communication History (PCH): Past communications History is a parameter measured based on the successful data collection and delivery of the same to BS in the previous intervals.

The decisions we are supposed to make here are classified into three. We want to classify an MDC as Non-Malicious (NM)or Malicious(M). Sometimes using the current values of the variables, it may not be possible to decide whether a node

is Non-malicious or Malicious. Therefore we are taking one more category called Unable to Decide (UD).

The overall working of this fuzzy-based decision-making to decide node as NM, M or UD is explained below:

1) The fuzzy rule R is derived by conducting experiments for TV, VI and PC values and the classifications required. The computed R is preloaded to respective CHs. The sample R we have used for the experiments is shown below:

$$R = \begin{bmatrix} 0.1 & 0.6 & 0.3 \\ 0.6 & 0.1 & 0.3 \\ 0.0 & 0.8 & 0.2 \end{bmatrix}$$

2) Every time BS deploys MDC, MDC is preloaded with values for TV, VI and PC during each interval, forming the factor vector r.
3) MDC visits CH and passes factor vector r to respective CH.
4) CH applies max-min composition with the rule matrix R using the received factor vector r. Evaluation vector e = roR is computed.
5) Decision-making using evaluation vector e is as follows: If scoring factors obtained in the form of e are distinct, the highest membership value decides the node's category and whether the MDC belongs to the category NM, M or UD. If MDC is classified as "NM", CH initiates the data transfer. If MDC is classified as "M" or "UD", second-level authentication using a public key cryptosystem is initiated.

2.3.2. ECC based on Second Level Authentication

This section will discuss the handshake mechanism used to authenticate MDC. This second-level authentication is invoked when the fuzzy method classifies the MDC as either "M" or "UD". Here for this authentication process, we assume that MDC and CH_i know each other's public key. The respective cluster head CH_i initiates the authentication process by sending a Nonce value and the current time TSi by encrypting it with PR_{CH_i} andPU_{MDC}. Upon receiving a non-malicious MDC having corresponding keys can decrypt the same. Then it increments the received Nonce to Nonce+1 and attaches a new timestamp value $T_{S_j}$and encrypts it using encrypted using PR_{MDC} and PU_{CH_i}. Upon receiving the reply from MDC, the cluster head CH_i decrypts and checks the received values to confirm that the MDC is authenticated. Also, to check the replay attack the received T_{S_j} value is verified. After verification, CH_j concludes that the MDC is Non-malicious and it initiates the data transfer. The message exchange between CH_i and MDC during the authentication process is illustrated below:

$$CH_i \rightarrow MDC : \{\{N_{once} \| T_{S_i}\}_{PR_{CH}}\}_{PU_{MDC}} \quad (1)$$

$$MDC \rightarrow CH_i : \left\{\{N_{once+1} \| T_{S_j}\}_{PR_{MDC}}\right\}_{PU_{CH_i}} \quad (2)$$

2.4. Data transfer by MDC to the Base Station

After two-level authentication, if a node is identified as Non-malicious, the respective cluster head CH_i encrypts the data M using the public key of the base station BS and constructs the following message M, PU_{BS}. The encrypted message is transferred to MDC, which carries the same to the base station BS. Before transferring the message to BS, MDC authenticates itself with BS by using the public and private keys of BS and its own. This authentication is initiated by BS as follows:

$$BS \rightarrow MDC : \{\{N_{once}\}_{PR_{BS}}\}_{PU_{MDC}} \quad (3)$$

$$MDC \rightarrow BS : \{\{N_{once+1}\}_{PR_{MDC}}\}_{PU_{BS}} \quad (4)$$

If MDC successfully manages this authentication, then BS will accept the collected data from MDC.

2.5. Updating Fuzzy Variables by BS for the Next Round

After completing one round, MDC visits the BS and, after authenticating itself, transfers the data to BS. From the time of deployment of MDC to transfer of data back to BS, completes one round of MDC. After successful data transmission, BS updates the fuzzy variable TV, VI and PCH for the next round. The updation is based on the results of the previous round. In the previous round, if the MDC has passed authentication at CH without entering the second level, i.e., just by the Fuzzy method, if the MDC was classified as Non-malicious, the current TV value will be increased by BS.

Based on the number of successful data transfers so far, VI and PCH values will be adjusted. The values of the fuzzy variables are tuned such that an MDC without entering second-level authentication at respective CH during the authentication process will have their values tuned such that in the next interval also, their probability of passing the authentication in the first level increases. The entire scheme explained in this section is summarized in 1; this flow diagram shows a single round of MDC from the deployment till it collects the data and transfers it securely at the BS.

3. Results and Discussion

Experiments are conducted to study the proposed scheme. For the given R matrix, we conducted experiments to see how the CH is going to classify an MDC as NM, M and UD for randomly selected vector r consisting of values of TV, V I and PCH. For every r, we applied max-min and computed e, and based on the computed e value node is classified. The experiments are repeated for randomly selected r, each time obtained e value, and the class to which the node belongs is recorded.

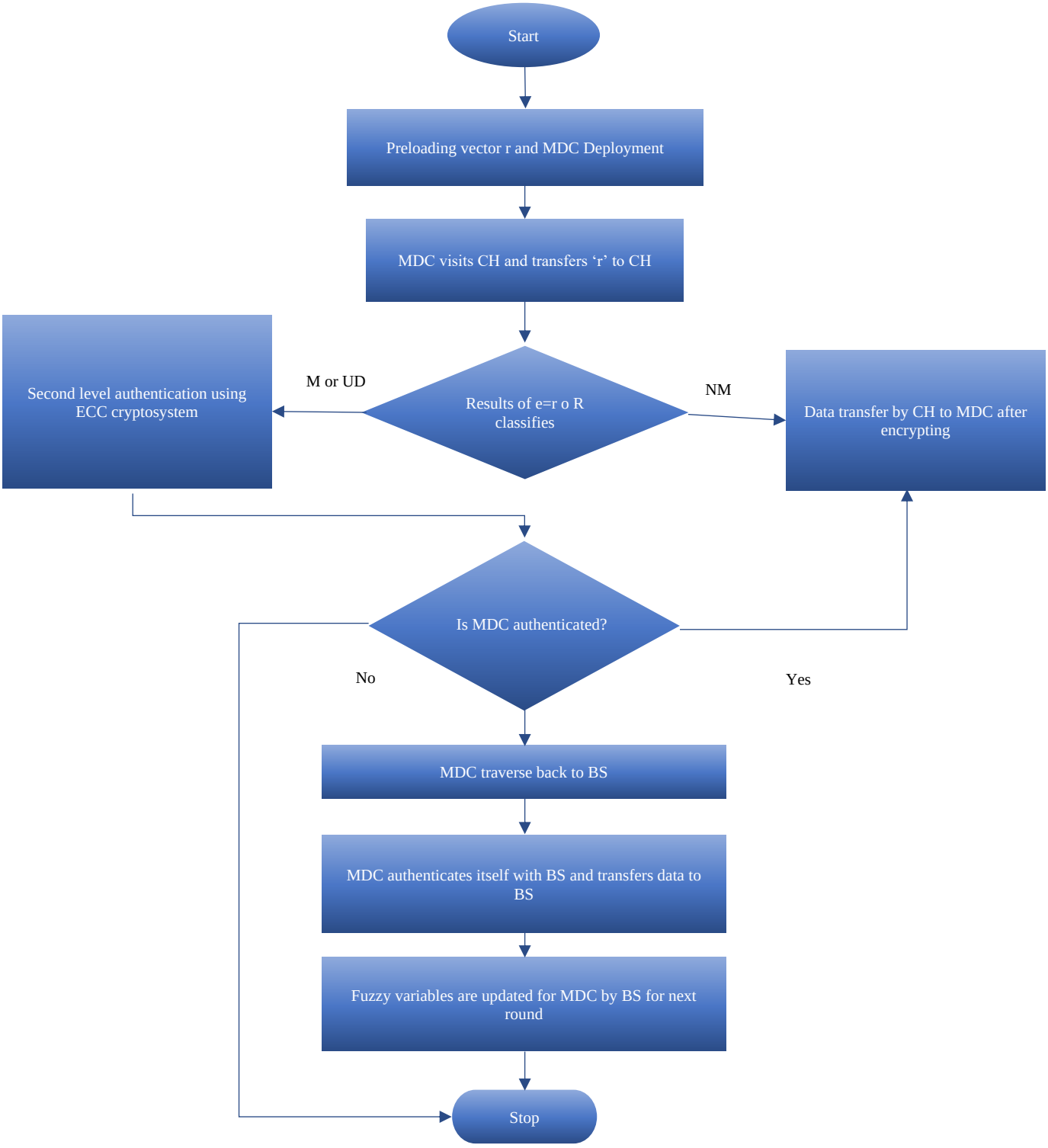

Fig. 1 Flow diagram illustrating one single round traversal of MDC visit during data collection

The results are tabulated. A few such recorded results are shown in Table 2. The experiments are repeated, and the graph is plotted for the outcome, i.e., the percentage of times the node is classified as NM without initiating second-level authentication. The graph is shown in 2. The recorded results show that around 50% of the time, it is possible to classify an MDC as Malicious by using just the Fuzzy method without the second-level authentication. One can expect this significant

benefit when dealing with resource-constrained environments like WSN, where saving energy consumption is crucial.

The next set of experiments is conducted to study the time complexity of the proposed scheme. For studying the scheme's time complexity, we have considered the complete authentication part starting from invoking the fuzzy method until the decision by CH to transfer the data or not to transfer.

Table 2. Sample recorded values after applying Max-Min

Tv	Vi	Pch	Class
0.7	0.9	0.1	Non-Malicious
0.5	0.2	0.4	Malicious
0.6	0.2	0.3	Malicious
0.9	0.7	0.1	Non-Malicious
0.3	0.2	0.9	Unable to Decide

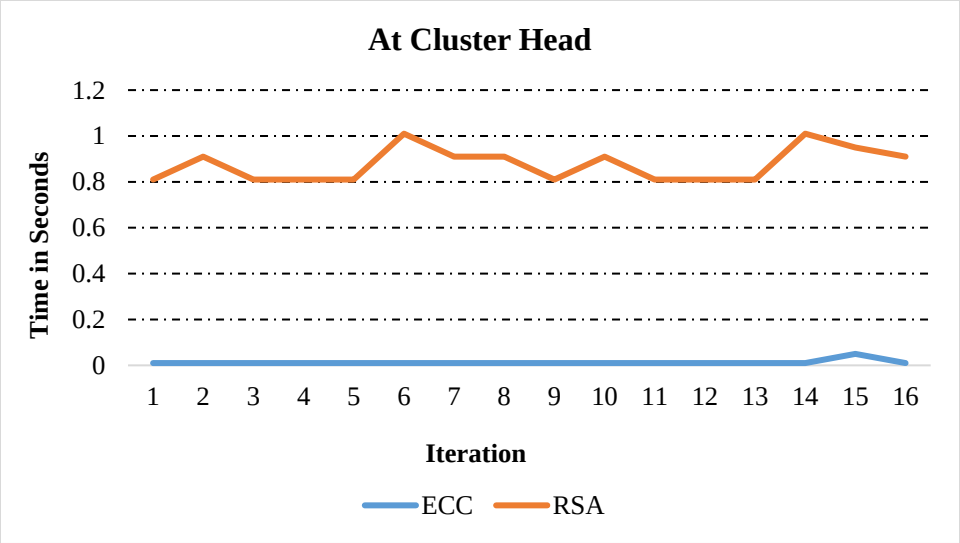

Fig. 2 Time Complexity recorded at Cluster Head considering both RSA and ECC cryptosystems

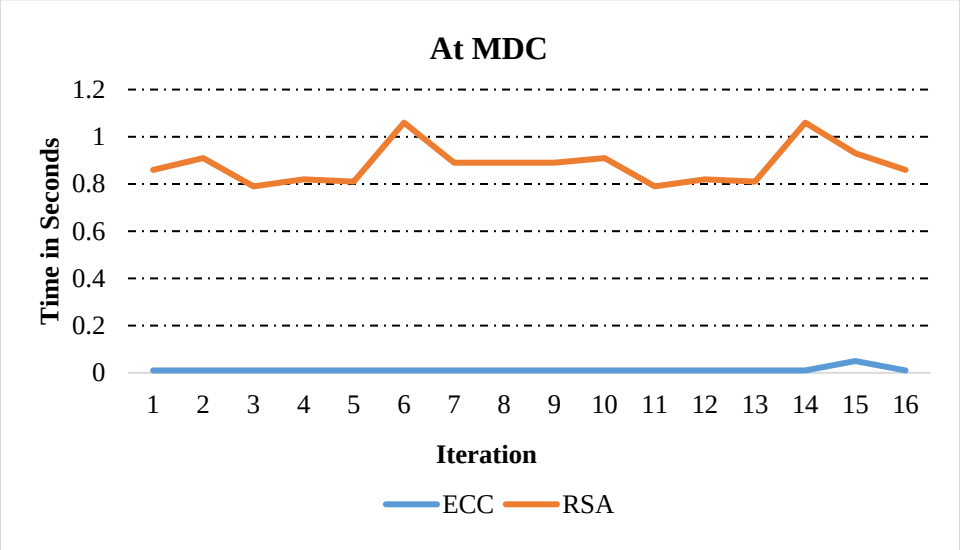

Fig. 3 Time complexity recorded at MDC considering both RSA and ECC cryptosystems

If the fuzzy method fails to classify the node, then the public key-based authentication scheme is invoked as the second level. For experimentation, we have considered both RSA and ECC-based public key cryptosystems. The first set of experiments is conducted wherein we use the RSA algorithm for second-level authentication. Time is recorded for the entire authentication process. Similar to the first set of experiments, we also repeated the experiment for randomly selected factor vector r and every iteration running time is recorded and tabulated. The next part of the experiments is conducted using an ECC-based public key cryptosystem for second-level authentication. Experiments are repeated for the

same set of randomly selected factor vectors using the ECC algorithm, and running times are recorded. A comparative graph illustrating the time complexity of the scheme recorded at cluster head CH using RSA and ECC public key cryptosystems is shown in 3.

Similarly, time complexity at MDC is recorded for the second-level authentication using RSA and ECC. The graph in 4 shows the execution time required by RSA and ECC algorithms for different iterations. Overall observation on time complexity illustrates that the ECC-based algorithm is computationally better than the RSA algorithm. Therefore, an ECC-based second-level authentication algorithm is suitable for resource-constrained networks like WSN. The performance analysis of RSA versus ECC has also studied which node belongs to are recorded. The results are tabulated. A few such recorded results are shown in Table 2. The experiments are repeated, and the graph is plotted for the outcome, i.e., the percentage of times the node is classified as NM without initiating second-level authentication. The graph is shown in 2. The recorded results show that around 50% of the time, it is possible to classify an MDC as Malicious by a fuzzy method without second-level authentication. One can expect this significant benefit when dealing with resource-constrained environments like WSN, where saving energy consumption is crucial. The next set of experiments is conducted to study the time complexity of the proposed scheme. For studying the scheme's time complexity, we have considered the complete authentication part starting from invoking the fuzzy method until the decision by CH to transfer the data or not to transfer. If the fuzzy method fails to classify the node, then the public key-based authentication scheme is invoked as the second level. For experimentation, we have considered both RSA and ECC-based public key cryptosystems. The first set of experiments is conducted wherein we use the RSA algorithm for second-level authentication. Time is recorded for the entire authentication process. Similar to the first set of experiments, we also repeated the experiment for randomly selected factor vector r and every iteration running time is recorded and tabulated. The next part of the experiments is conducted using an ECC-based public key cryptosystem for second-level authentication. Experiments are repeated for the same set of randomly selected factor vectors using the ECC algorithm, and running times are recorded. A comparative graph illustrating the time complexity of the scheme recorded at cluster head CH using RSA and ECC public key cryptosystems is shown in the literature [33]. Based on this literature, we experimented with RSA and ECC and concluded that ECC is suitable for WSN applications.

4. Conclusion

We have addressed Secure Data collection using Mobile Data Collector in this work. The proposed scheme ensures the confidentiality of the data from the time the sensor node senses it till it reaches the BS. We use a lightweight authentication scheme comprising two levels to identify malicious MDC. The first level uses Fuzzy logic to classify a node. The fuzzy method classifies a node into one of the three classes Non-malicious, Malicious or Unable to Decide. If the fuzzy method classifies an MDC as either Malicious or Unable to Decide, second-level authentication using ECC public key cryptosystem is used to confirm whether the node is indeed Malicious. If this second level identifies the MDC as malicious, sensed data is not transferred to MDC. Both issues are addressed efficiently using lightweight cryptographic algorithms like symmetric keys and ECC-based public key cryptosystems. Experimental results conclude that during multiple MDC visits for data collection, around 50% of the time, it is possible to authenticate an MDC just by using fuzzy logic, which is considered an energy-efficient method compared to the use of compute-intensive cryptographic algorithms. We have also conducted experiments to check the computation overhead incurred for authentication if second-level authentication is invoked. For this study, we considered RAS and ECC public key cryptosystems. The recorded results show that ECC-based cryptosystems efficiently compute overhead on cluster head and MDC. In conclusion, we can say that the proposed scheme increases the overall network lifetime as we use MDC for data collection and, wherever possible, lightweight methods to achieve security.

References

[1] Ari A.A.A, Gueroui A, Labraoui N and Yenke B.O, “Concepts and Evolution of Research in the Field of Wireless Sensor Networks,” *International Journal of Computer Networks & Communications,* vol. 7, no. 1, pp. 81-98, 2015. Crossref, https://doi.org/10.48550/arXiv.1502.03561

[2] Rawat P, Singh K.D, Chaouchi H and Bonnin J.M, “Wireless Sensor Networks: A Survey on Recent Developments and Potential Synergies,” *The Journal of Supercomputing,* vol. 68, pp. 1-48, 2014. Crossref, https://doi.org/10.1007/s11227-013-1021-9

[3] Srinivasa Rao, P.C. and Banka H, “Energy Efficient Clustering Algorithms for Wireless Sensor Networks: Novel Chemical Reaction Optimization Approach,” *Wireless Networks,* vol. 23, pp. 433-452, 2017. Crossref, https://doi.org/10.1007/s11276-015-1156-0

[4] Pratyay Kuila and Prasanta K. Jana, “A Novel Differential Evolution Based Clustering Algorithm for Wireless Sensor Networks,” *Applied Soft Computing,* vol. 25, pp. 414-425, 2014. Crossref, https://doi.org/10.1016/j.asoc.2014.08.064

[5] Liu Y, Xiong N, Zhao Y, Vasilakos A. V, Gao J and Jia Y, “Multi-Layer Clustering Routing Algorithm for Wireless Vehicular Sensor Networks,” *IET Communications,* vol. 4, no. 7, pp. 810-816, 2010 Crossref, https://doi.org/10.1049/iet-com.2009.0164

[6] Mann P.S and Singh S, "Improved Metaheuristic Based Energy-Efficient Clustering Protocol for Wireless Sensor Networks," *Engineering Applications of Artificial Intelligence,* vol. 57, pp. 142-152, 2017. Crossref, https://doi.org/10.1016/j.engappai.2016.10.014

[7] Diongue D and Thiare O, "ALARM: An Energy Aware Sleep Scheduling Algorithm for Lifetime Maximization in Wireless Sensor Networks," In *Proceedings of the 2013 IEEE Symposium on Wireless Technology and Applications (ISWTA)*, Kuching, Malaysia, pp. 74-79, 2013. Crossref, https://doi.org/10.1109/ISWTA.2013.6688821

[8] Li G, Chen H, Peng S, Li X, Wang C, Yu S and Yin P, "A Collaborative Data Collection Scheme Based on Optimal Clustering for Wireless Sensor Networks," *Sensors,* vol. 18, no. 8, pp. 2487, 2018. Crossref, https://doi.org/10.3390/s18082487

[9] Randhawa S and Jain S, "Data Aggregation in Wireless Sensor Networks: Previous Research, Current Status and Future Directions," *Wireless Personal Communications,* vol. 97, pp. 3355-3425, 2017. Crossref, https://doi.org/10.1007/s11277-017-4674-5

[10] Jung W. S, Lim K. W, Ko Y. B and Park S. J, "Efficient Clustering-Based Data Aggregation Techniques for Wireless Sensor Networks," *Wireless Networks,* vol. 17, no. 5, pp. 1387-1400, 2011. Crossref, https://doi.org/10.1007/s11276-011-0355-6

[11] Paul, T., Stanley and K. G, "Data Collection from Wireless Sensor Networks Using a Hybrid Mobile Agent Based Approach," In *Proceedings of the 2014 IEEE 39th Conference on Local Computer Networks (LCN2014)*, pp. 288-295, 2014. Crossref, https://doi.org/10.1109/LCN.2014.6925783

[12] Gupta G. P, Misra M and Garg K, "Energy and Trust-Aware Mobile Agent Migration Protocol for Data Aggregation in Wireless Sensor Networks," *Journal of Network and Computer Applications,* vol. 41, pp. 300-311, 2014. Crossref, https://doi.org/10.1016/j.jnca.2014.01.003

[13] Dong M, Ota K, Yang L. T, Chang S, Zhu H and Zhou Z, "Mobile Agent-Based Energy-Aware and User Centric Data Collection in Wireless Sensor Networks," *Computer Networks,* vol. 74, pp. 58-70, 2014. Crossref, https://doi.org/10.1016/j.comnet.2014.06.019

[14] Ang K.L.M, Seng J.K.P and Zungeru A.M, "Optimizing Energy Consumption for Big Data Collection in Large-Scale Wireless Sensor Networks With Mobile Collectors," *IEEE Systems Journal,* vol. 12, no. 1, pp. 616-626, 2018. Crossref, https://doi.org/10.1109/JSYST.2016.2630691

[15] Takaishi D, Nishiyama H, Kato N and Miura R, "Toward Energy Efficient Big Data Gathering in Densely Distributed Sensor Networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 2, no. 3, pp. 388-397, 2014. Crossref, https://doi.org/10.1109/TETC.2014.2318177

[16] Di Francesco M, Das S.K and Anastasi G, "Data Collection Wireless Sensor Networks with Mobile Elements: A Survey," *ACM Transactions on Sensor Networks (TOSN),* vol. 8, no. 1, pp. 1-31, 2011. Crossref, https://doi.org/10.1145/1993042.1993049

[17] Yogeswari R and Subathra V, "A Survey on Efficient Data Collection in Wireless Sensor Networks," *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 1, no. 9, pp. 2181, 2013.

[18] Eti Walia, Vinay Bhatia and Gurdeep Kaur, "Detection of Malicious Nodes in Flying Ad-HOC Networks (FANET)," *SSRG International Journal of Electronics and Communication Engineering*, vol. 5, no. 9, pp. 6-12, 2018. Crossref, https://doi.org/10.14445/23488549/IJECE-V5I9P102

[19] Poornima A. S, and B. B. Amberker, "Secure Data Collection using Mobile Data Collector in Clustered Wireless Sensor Networks," *IET Wireless Sensor Systems,* vol. 1, no. 2, pp. 85-95, 2011. Crossref, https://doi.org/10.1049/iet-wss.2010.0086

[20] Puthal, Deepak and Bibhudatta Sahoo, "Secure Data Collection and Critical Data Transmission in Mobile Sink WSN," *Secure and Energy-Efficient Data Collection Technique*, 2012.

[21] Renold, A. Pravin, and A. Balaji Ganesh, "Energy Efficient, Secure Data Collection with Path-Constrained Mobile Sink in Duty-Cycled Unattended Wireless Sensor Network," *Pervasive and Mobile Computing,* vol. 55, pp. 1-12, 2019. Crossref, https://doi.org/10.1016/j.pmcj.2019.02.002

[22] Rajesh, D. Hevin, and B. Paramasivan, "Fuzzy Logic Based Performance Optimization with Data Aggregation in Wireless Sensor Networks," *Procedia Engineering*, vol. 38, pp. 3331-3336, 2012. Crossref, https://doi.org/10.1016/j.proeng.2012.06.385

[23] Yang, Hongyu, Xugao Zhang and Fang Cheng, "A Novel Algorithm for Improving Malicious Node Detection Effect in Wireless Sensor Networks," *Mobile Networks and Applications*, vol. 26, pp. 1564-1573, 2021. Crossref, https://doi.org/10.1007/s11036-019-01492-4

[24] Prathap, U., P. Deepa Shenoy and K. R. Venugopal, "CMNTS: Catching Malicious Nodes with Trust Support in Wireless Sensor Networks," In *2016 IEEE Region 10 Symposium (TENSYMP), IEEE*, pp. 77-82, 2016. Crossref, https://doi.org/10.1109/TENCONSpring.2016.7519381

[25] Nadeem, Aamer and M. Younus Javed, "A Performance Comparison of Data Encryption Algorithms," In *2005 International Conference on Information and Communication Technologies, IEEE*, pp. 84-89. 2005. Crossref, https://doi.org/10.1109/ICICT.2005.1598556

[26] Doomun, M. Razvi and K. M. S. Soyjaudah, "Analytical Comparison of Cryptographic Techniques for Resource-Constrained Wireless Security," *International Journal of Network Security*, vol. 9, no. 1, pp. 82-94, 2009.

[27] Kapoor, Vivek, Vivek Sonny Abraham and Ramesh Singh, "Elliptic Curve Cryptography," *Ubiquity*, vol. 9 no. 20, pp. 1-8, 2008. Crossref, https://doi.org/10.1145/1386853.1378356

[28] Wang F and Liu, J, "Networked Wireless Sensor Data Collection: Issues, Challenges, and Approaches," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4, pp. 673-687, 2011. Crossref, https://doi.org/10.1109/SURV.2011.060710.00066

[29] Korada Kishore Kumar and Konni Srinivasa Rao, "An Efficient users Authentication and Secure Data Transmission of Cluster-based Wireless Sensor Network," *SSRG International Journal of Computer Science and Engineering*, vol. 5, no. 1, pp. 1-5, 2018. Crossref, https://doi.org/10.14445/23488387/IJCSE-V5I1P101

[30] Shu, Tao, Marwan Krunz, and Sisi Liu, "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes," *IEEE Transactions on Mobile Computing*, vol. 9, no. 7, pp. 941-954, 2010. Crossref, https://doi.org/10.1109/TMC.2010.36

[31] Zhang, Ping, Shaokai Wang, Kehua Guo and Jianxin Wang, "A Secure Data Collection Scheme Based on Compressive Sensing in Wireless Sensor Networks," *Ad Hoc Networks*, vol. 70, pp. 73-84, 2018. Crossref, https://doi.org/10.1016/j.adhoc.2017.11.011

[32] W.R.Heinzelman, A.Chandrakasan, and H.Balakrishnan, "Energy Efficient Communication Protocol for Wireless Micro Sensor Networks," In *Proceedings of IEEE Hawaii International Conference on System Sciences*, vol. 2, pp. 10, 2000. Crossref, https://doi.org/10.1109/HICSS.2000.926982

[33] Dindayal Mahto and Dilip Kumar Yadav, "Performance Analysis of RSA and Elliptic Curve Cryptography," *International Journal of Network Security*, vol. 20, no. 4, pp. 625-635, 2018. Crossref, https://doi.org/10.6633/IJNS.201807

[34] Jain S, Shah R.C, Brunette W and Borriello G, Roy S, "Exploiting Mobility for Energy Efficient Data Collection in Wireless Sensor Networks," *Mobile Networks and Applications*, vol. 11, pp. 327-339, 2006. Crossref, https://doi.org/10.1007/s11036-006-5186-9

[35] Mukherjee R, Roy S and Das A, "Survey on Data Collection protocols in Wireless Sensor Networks using Mobile Data Collectors," In *Proceedings of the IEEE 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, pp. 632-636, 2015.