An Efficient Source Anonymity Technique based on Exponential Distribution against a Global Adversary Model using Fake Injections

Anas Bushnag
School of Engineering
University of Bridgeport
CT, USA
abushnag@my.bridgeport.edu

Abdelshakour Abuzneid
School of Engineering
University of Bridgeport
CT, USA
abuzneid@bridgeport.edu

Ausif Mahmood
School of Engineering
University of Bridgeport
CT, USA
mahmood@bridgeport.edu

ABSTRACT

The security of Wireless Sensor Networks (*WSNs*) is vital in several applications such as the tracking and monitoring of endangered species such as pandas in a national park or soldiers in a battlefield. This kind of applications requires the anonymity of the source, known as Source Location Privacy (*SLP*). The main aim is to prevent an adversary from tracing back a real event to the originator by analyzing the network traffic. Previous techniques have achieved high anonymity such as Dummy Uniform Distribution (*DUD*), Dummy Adaptive Distribution (*DAD*) and Controlled Dummy Adaptive Distribution (*CAD*). However, these techniques increase the overall overhead of the network. To overcome this shortcoming, a new technique is presented: Exponential Dummy Adaptive Distribution (*EDAD*). In this technique, an exponential distribution is used instead of the uniform distribution to reduce the overhead without sacrificing the anonymity of the source. The exponential distribution improves the lifetime of the network since it decreases the number of transmitted packets within the network. It is straightforward and easy to implement because it has only one parameter λ that controls the transmitting rate of the network nodes. The conducted adversary model is global, which has a full view of the network and is able to perform sophisticated attacks such as rate monitoring and time correlation. The simulation results show that the proposed technique provides less overhead and high anonymity with reasonable delay and delivery ratio. Three different analysis models are developed to confirm the validation of our technique. These models are visualization model, a neural network model, and a steganography model.

KEYWORDS

WSNs Privacy; Source Location Privacy; Context Privacy.

1 INTRODUCTION

WSNs consist of homogeneous, small, and independent sensor nodes [1]. These sensors are connected wirelessly to create a functional network. They are deployed in areas of interest to sense global phenomena such as temperature or humidity [2]. Moreover, they can be used in tracking and monitoring applications [17]. For example, when a node detects a real event, this node becomes the source node. Whereas other nodes act as forwarders to transmit the event towards the sink node until it is finally delivered [3]. Commonly, the sink node has more capabilities and resources such as the processing computation and energy than the ordinary nodes. *WSNs* is also involved in many tracking and monitoring applications such as animal, patient, or border surveillance [4]. Security in *WSNs* is a real challenge due to the limitations of the resources in sensor nodes [18].

Security is categorized into content and context [5]. Content security is to prevent the adversary from exposing the content of packets. This can be achieved by using the current encryption techniques including confidentiality, authentication, and integrity. On the other hand, context is all about hiding the location of the source or the sink node [6]. The adversary should not be able to trace back the real event to the source node [7]. Context is harder to counter because even if the network uses the most advanced encryption techniques, the source or the sink node are vulnerable to adversary attacks that are based on traffic analysis [8-9,19] such as rate monitoring and time correlation. Therefore, different techniques must be employed.

The type of attacks performed against *WSNs* depends on the type of the adversary. A local adversary with a partial view of the network and limited resources is not capable of applying sophisticated attacks [10]. In contrast, a global adversary that has a full view of the network and sufficient resources can perform advanced attacks such as rate monitoring and time correlation [11-12].

Q2SWinet'17, November 21-25, 2017, Miami, FL, USA
© 2017 Association for Computing Machinery.
ACM ISBN 978-1-4503-5165-2/17/11...$15.00.
DOI: http://dx.doi.org/10.1145/3132114.3132120

There are several ways to counter a global adversary such as separate path routing, network location anonymization, network coding, and dummy data sources. Separate Path Routing (*SPR*) generates different paths from origin to sink, which means packets of an event using various routes to the destination. Network Location Anonymization hides the identity of the source through pseudonyms. Network Coding breaks a packet into smaller pieces. These pieces follow different routes to the sink. Dummy Data Sources generates dummy sources, which create fake traffic to hide the real traffic inside. Dummy Data Sources is used in the proposed technique in this paper since it provides higher anonymity than other approaches. The exponential distribution is employed in the proposed technique because of its simplicity and flexibility. It has only one parameter λ which controls the transmission rate. Moreover, exponential distribution reduces the overhead compared to the uniform distribution used in previous techniques. The exponential distribution determines the time duration between events. It is a continuous probability distribution that uses Poisson technique to predict the occurrence of the next event. The mean and standard deviation of the exponential distribution are the same, which is $\frac{1}{\lambda}$ [13]. The exponential distribution is based on the Poisson distribution. For instance, if a random variable follows the Poisson distribution with the occurrence rate of 4, the same random variable can follow the exponential λ distribution with a mean and standard deviation of $\frac{1}{\lambda} = \frac{1}{4} = 0.25$. Generally, the exponential distribution increases the lifetime of the network compared to the uniform distribution. Moreover, it is simplest and more manageable than the normal distribution, which has more than one parameters. The use of the exponential distribution in the proposed technique improves the overall performance of the network.

The rest of the paper is organized as the following. Section 2 describes the related work. Section 3 presents the system models. Section 4 discusses the proposed technique. Section 5 presents the simulation and results. Section 6 describes the anonymity analysis models. Section 7 presents the conclusion.

2 RELATED WORK

A recent research in addressing source anonymity against a global adversary is reported in [14-15] where three techniques are developed. Dummy Uniform Distribution technique (*DUD)* [14-15] injects the network with fake packets to mislead the adversary about the presence of the real event. It reduces the overhead caused by the fake packets by using probability. The notion is to divide the network into equal time intervals. All sensor nodes have to transmit real or fake packets by the end of the interval to avoid any time correlation attack by the adversary. If a node detects an asset, it creates a real event; then this event is sent by the end of the interval based on probability. In case a node does not have a real packet to send, it generates and sends a fake packet using probability instead. When a node receives a real packet, it forwards the packet to the next node on the path towards the sink using the same probability technique. However, if a node receives a fake packet, it drops the packet instantly. Since all nodes transmit using probability, each node will have its pattern of sending intervals, which confuses the adversary about the presence of the real event. A probability can be defined as a random number between 0 and 1. If the thrown random number is less than the predefined transmission rate for example 0.2, the node transmits its real or fake packet. However, if the thrown number is larger than the threshold, it tries to transmit the packet in the following interval. This process is repeated until the event is received by the sink. Since this technique does not guarantee the maximum delay, Dummy Adaptive Distribution (*DAD)* [14-15] is introduced. It categorizes the network nodes into real and fake nodes. All nodes are considered fake at the beginning of the network lifetime. Fake nodes will follow the same process as *DUD*. However, if a node detected a real event or forwarding a previously received real event packet, it becomes a real node. Real nodes will increase their transmitting rate by a specific value to give an advantage to the real packets over the fake ones. Once, the node transmits its real packets; it reduces its original transmitting rate by the same specific value. This is crucial to make the average transmitting rate of the real nodes equal to the fake nodes causing more obscure to the adversary. Hence, the adversary will not notice the existence of the real event. Even though *DAD* performs much better than *DUD* regarding delay and delivery ratio, it is still unable to fully guarantee the maximum delay. Thus, Controlled Dummy Adaptive Distribution (*CAD)* [14-15] is developed to meet the maximum delay required by the application. It is based on *DAD*, but it forces the node to transmit its real packet after n-consecutive intervals (set the transmission rate to 1). Increasing the maximum waiting intervals before transmitting provides more delay and higher anonymity whereas decreasing the maximum waiting intervals provides less delay and lower anonymity. It can be considered as a trade-off between latency and privacy.

In [10], A. Basel and C. Andrew have claimed that the anonymity of *WSNs* should be measured by the amount of information about the real event's time and location. This can be argued because the authors assume that the adversary already knows the presence of the real event. However, in the proposed model, the adversary is assumed not to know the existence of the real event nearby a sensor node at a certain time, which is more realistic. Therefore, if we can confuse the adversary about the presence of the real event, this will automatically lead to a time and location privacy for the real event.

In [12,19], *FitProbRate* uses exponential distribution to predict the time of the next interval. Then, it runs Anderson-Darling test (*A-D*) every time a real event is detected, which causes high overhead. *A-D* is used to test if the sequence of packets follows the exponential distribution or not. *FitProbRate* uses the result of the *A-D* to determine if the system provides a high level of anonymity. This is debatable because the anonymity of a system is affected by many factors such as time correlation and rate monitoring plus the type of distribution.

3 SYSTEM MODELS

In this section, the system models are presented including the network model, routing model, adversary model, and anonymity model.

3.1 Network Model

A *WSN* consists of several sensor nodes is placed in an area of interest such as a vast forest to monitor the location of a panda. The main aim is to prevent a global adversary from locating the panda by analyzing the network traffic. Sensor nodes can be deployed randomly or in specific locations. When a node detects a panda, it transmits the location of the panda to the sink node throughout the intermediate nodes. The sink node can be placed in any location within the network boundaries. All nodes fall within the sensing range of a transmitting node are considered as neighbors to this node. The sensors can locate themselves using *GPS* or one of the localization techniques. The time of the network is divided into intervals. Communications between nodes are assumed to be encrypted and secure. Real and fake packets are identical in terms of size and structure to avoid any size or structure correlation attacks from the adversary. Nodes have the ability to distinguish the real packets from the fake ones.

3.2 Routing Model

The routing protocol is location-based, which selects the shortest path towards the sink. In this type of routing protocols, all nodes need to be informed about their coordinates and their neighbors' coordinates. The used routing protocol is adjustable to any failure of the network nodes. For instance, if a node is damaged or running out of battery, the routing protocol will select the second closest node towards the sink. The flooding routing protocol is not used to reduce the overall overhead of the network.

3.3 Adversary Model

The adversary model employed is the global adversary because it is harder and more challenging to counter. This is similar to the passive, external and global adversary model presented in [8,11-12,19]. The adversary is capable of deploying its own nodes to monitor the desired *WSN*. The adversary can perform sophisticated analysis such as rate monitoring and time correlation. However, more assumptions are added to provide the adversary with more advanced features. It has the ability to create a data set of the observed intervals for each node in the network. This data set can be fed into a neural network to disclose the presence of the real event. Furthermore, the adversary can visualize the data set and detect any suspicious patterns that might lead to the existence of the real event.

3.4 Anonymity Model

The anonymity of the system and how secure it is, can be calculated using the following steganography equation [16]:

$$\boldsymbol{d(\alpha,\beta) = \alpha \log_2 \frac{\alpha}{1-\beta} + (1-\alpha)\log_2 \frac{1-\alpha}{\beta}} \tag{1}$$

where $\boldsymbol{\alpha}$ is the probability of the adversary to falsely detect the real event. It is the false positive of the system, which means the possibility of the adversary to say there is e.g. a panda, and actually, there is no panda. Whereas $\boldsymbol{\beta}$ is the probability of the adversary to not detect the presence of the real event. It is the false negative of the system, which means the possibility of the adversary to say there is no e.g. panda, and actually, there is a panda. Additionally, the system should follow this rule: $\boldsymbol{d(\alpha,\beta) \le \varepsilon}$ in order to be secure where $\boldsymbol{d(\alpha,\beta)}$ is the anonymity level provided by a specific technique (it can be considered as the threshold of the system) and $\boldsymbol{\varepsilon}$ is the anonymity level required by the application.

4 PROPOSED TECHNIQUE

To reduce the overhead of a network without sacrificing the privacy of the source node, Exponential Dummy Adaptive Distribution (*EDAD*) is introduced. It uses two types of packets: real and fake. Real packets contain the actual information of the real event whereas fake packets are deployed to mislead the adversary about the location of the real event. Real and fake packets are identical in terms of size and structure to avoid any size/structure correlation attacks. The exponential distribution has only one parameter$\boldsymbol{\lambda}$, which represents the transmitting rate. Accordingly, this can be an advantage because it helps to fix the rate of all nodes' flows in the network. Therefore, the adversary is unable to distinguish the difference between real and fake events. However, each node still has its own sending interval pattern as it is based on a probability. The next sending interval can be obtained from the following equations:

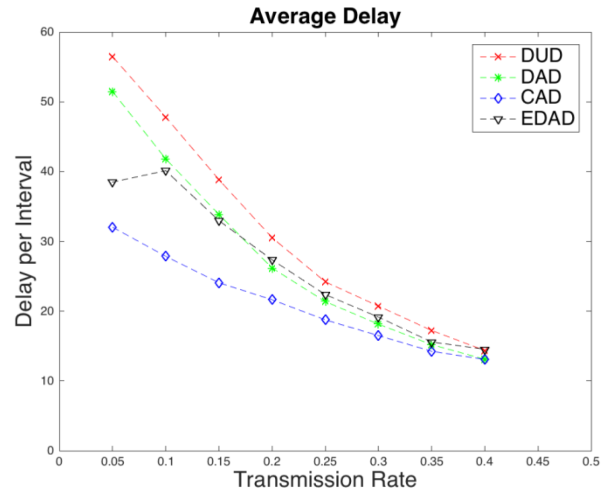
$$\boldsymbol{p = e^{-\lambda t}} \tag{2}$$

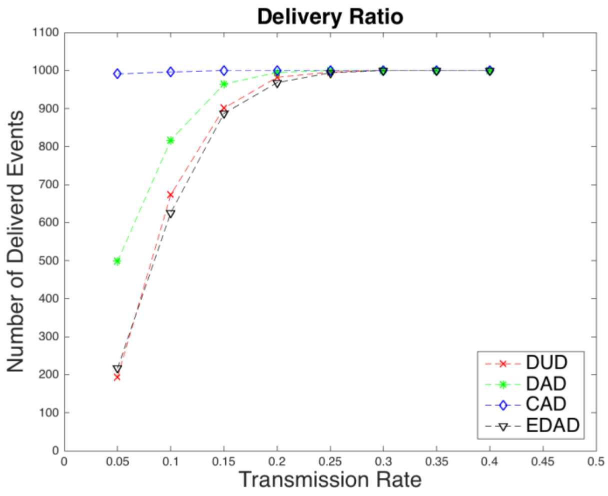
$$\boldsymbol{t = \frac{\ln p}{-\lambda}} \tag{3}$$

Where $\boldsymbol{p}$ is the probability, $\boldsymbol{\lambda}$ is the transmitting rate, and $\boldsymbol{t}$ is the next sending interval time. Each Node implements equation 3 whenever it has a packet in its buffer to send whether the packet type is real or fake. If there is no real event, nodes keep sending fake packets using equation 3. Once a node detects a real event, it creates and starts transmitting the real packets. The next scheduled fake packet is replaced by the real one. This is necessary not to violate the exponential distribution sequence. Further, it decreases the chances of an adversary to detect the real event by applying time correlation attacks. Since all nodes using the same value of $\boldsymbol{\lambda}$, and each node has a different sending interval pattern, the adversary will be confused about the existence of the real event.

5 SIMULATION AND RESULTS

In the simulation, 25 sensor nodes are deployed in an area of interest, 600 m by 600 m. The lifetime of the network is selected to be 100 intervals. The purpose of the *WSN* is to track and monitor the movement of a panda. The network has one sink node on the right side of it. Whenever a node detects a panda, it informs the sink about the current location of the panda throughout the intermediate nodes. The tested exponential transmission rates are 0.05, 0.1, 0.15, 0.2, 0.25, 0.3, 0.35, and 0.4. One node only detects the panda. Each transmission rate is evaluated under one-thousand random cases. Each case has a random location and starting interval between 0 and 49 for the panda. A comparison between *EDAD*, *DUD*, *DAD*, and *CAD* is conducted regarding average delay, average overhead, and delivery ratio. The proposed technique is implemented in a specialized simulator using C#.





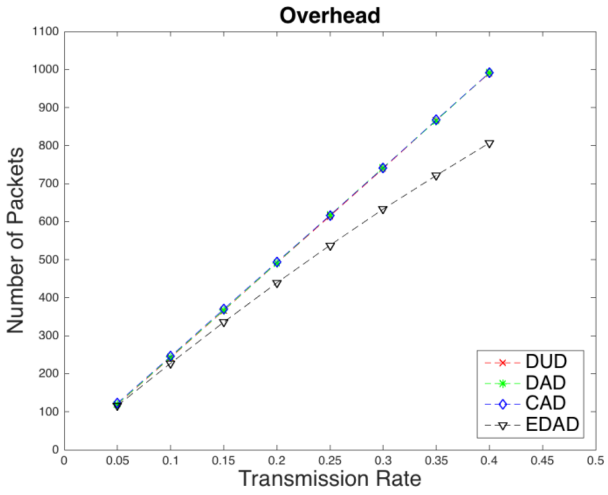


Figure 1: Average Delay, Delivery Ratio, and the Overhead.

As shown in Fig. 1, *EDAD* reduces the overhead compared to other techniques. It decreases the number of overhead packets whenever the rate increases. This indicates that *EDAD* can be used at higher rates, which increases the delivery ratio and decreases the delay subsequently. However, the performance of the *EDAD* in terms of average delay is very similar to *DAD* and is not as good as *CAD*. This is because *EDAD* reduces the overhead by using the exponential distribution, which in return does not guarantee the maximum delay of the event. The *CAD* technique provides a high delivery ratio in low and high rates because it uses a specific mechanism that forcing the node to transmit its real packet after a predefined number of intervals. However, this could lead to a privacy problem because it violates the uniform distribution sequence. The *EDAD* technique performs similarly at high rates. However, at low rates, the number of delivered packets is decreased because of the delay caused by the exponential distribution. In conclusion, *EDAD* reduces the overhead but it increases the delay while keeping a high level of anonymity. Whereas, *CAD* increases the overhead and decreases the delay within an acceptable level of anonymity.

6 ANONYMITY ANALYSIS

In this section, three models are developed to verify the validation of the proposed technique; they prove that our technique provides a reasonable delay, delivery ratio, and reduced overhead without sacrificing the privacy of the source node. These models are visualization, neural network, and steganography. They are applicable to any anonymity technique whenever the transmissions between nodes in the network are available. Specifically, during the simulation lifetime intervals, some nodes transmit packets, and some nodes do not. When a node transmits a packet; it is represented by a binary value of 1 whereas if the node does not transmit a packet; it is represented by a binary value of 0. As a result, the output of the simulation is a binary matrix. Columns indicate the node number and rows indicate the interval number. These models examine the time correlation, rate monitoring, and the distribution type of a system to determine the level of anonymity the proposed technique provides. Analysis models were developed using MATLAB2014b.

6.1 Visualization Model

In this model, the simulation output is converted into a binary image. Ones are represented as black pixels and zeros are represented as white pixels. Another binary image is created with cases using only fake events. The aim is to compare the output binary image of the real events to the binary image of the fake ones. If they are similar and have no differences, that means the proposed technique is secure and valid. However, if the real events' binary image has visible or suspicious patterns, this indicates the presence of the real event nearby a sensor node at a certain time, which means the developed technique is weak in terms of anonymity. The *EDAD* technique is tested using a selected transmission rate of 0.2 and compared to an entire random output that uses the same rate and distribution as shown in Fig. 2.

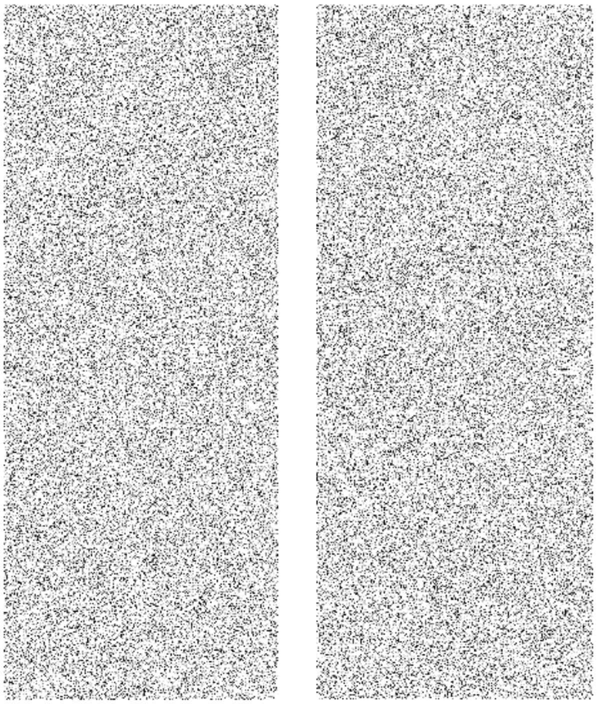


Figure 2: The left binary image is the real cases. The right binary image is the fake random cases.

As shown in Fig. 2, both images are almost identical, which for sure confuses the adversary about the existence of the real events. The adversary cannot tell which one has the real event and which one does not. This increases the uncertainty, which is required by most of the applications. Moreover, the proposed technique does not generate any visible or suspicious patterns that could lead to the source of the real event.

6.2 Neural Network Model

This model feeds the output binary matrix of the simulation into a neural network to see if the neural network can differentiate between real and fake cases. If the neural network is confused about the presence of the real event, this would mean that the proposed technique is secure and provides high anonymity. Two thousand random scenarios are created. One thousand scenarios represent our solution and the other thousand scenarios represent random cases with only fake packets. The *WSN* has 25 nodes and the number of intervals is 100. Therefore, each scenario will have 2500 inputs that feed into the neural network. *W* is the weights that are created by the neural network, *b* is the bias and is a constant. At the first run of the neural network, weights are generated randomly. Then, a gradient descent algorithm is implemented to reduce the gap between the actual output and expected output by finding the best weights combination. Two scenarios have been created, one without a validation set and the other uses a validation set of the training data to avoid overfitting. An overview of the neural network is shown in Fig. 3.

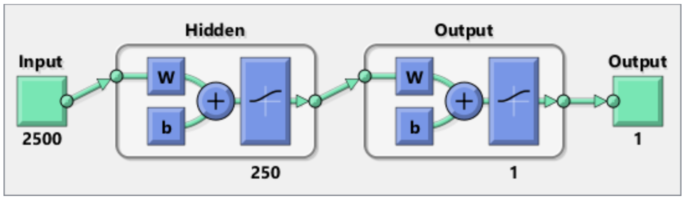


Figure 3: Neural Network Architecture.

The proposed technique is evaluated at a transmission rate of 0.1. The number of neurons in the hidden layer is 250. The back propagation algorithm is gradient descent, and the used activation function is sigmoid for both hidden and output layers. The output layer has only one neuron, it produces a 1 if there is a real event and 0 otherwise.

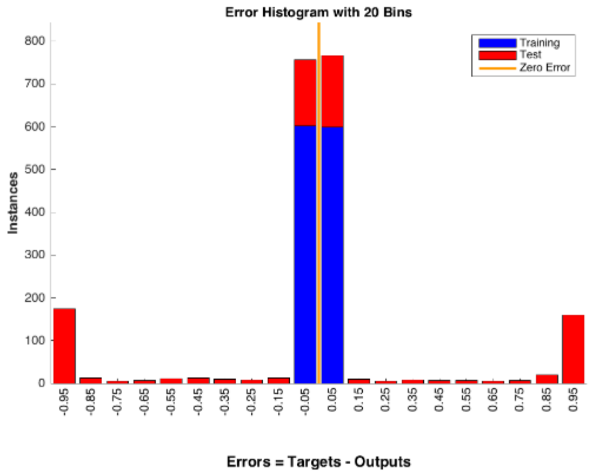


Figure 4: *EDAD* with a rate of 0.1 (without a validation set).

In the first scenario (without a validation set). The date set is categorized into only training and testing data as shown in Fig. 4. The blue columns represent Training date and the red columns represent testing date. The error of the training data, which is the difference between the actual output and expected output is almost zero. This indicates that the neural network is trained properly. On the other hand, the error of the testing data is very high and it is around 50 percent because the testing date is divided between 0 and 1, which indicates the neural network is still confused about the presence of real events even after the network is trained properly. This shows that the proposed solution provides high anonymity.

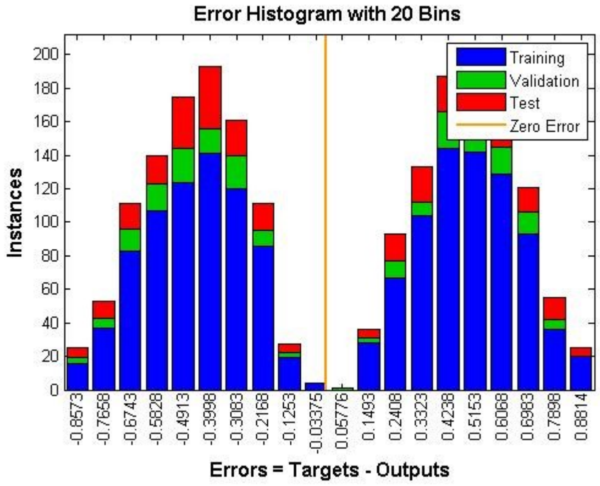


Figure 5: *EDAD* with a rate of 0.1 (with a validation set).

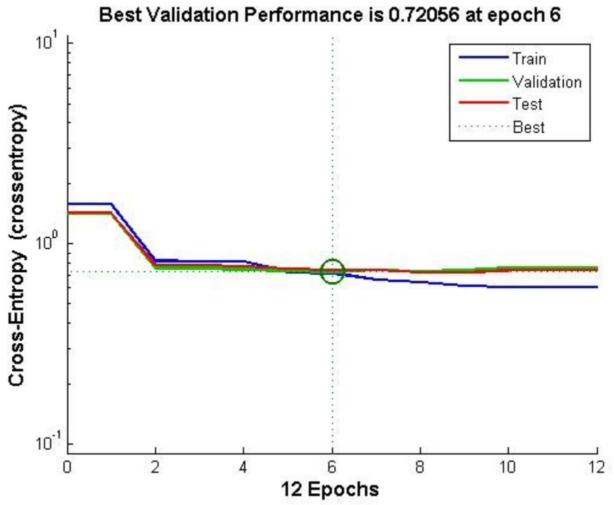


Figure 6: Performance of *EDAD* (with a validation set)

Someone can argue that in the first scenario, a validation set is not used on purpose, and may reduce the generalization of the network. Therefore, another scenario is introduced. In the second scenario (with a validation set) as shown in Fig. 5 the network cannot achieve 100% accuracy or zero error on the training data set (Error Histogram) since the accuracy is not improving on the validation data sets (represented by the green columns). After 12 epochs, the network has an early stop to avoid overfitting of the network (Fig. 6). This is because the large amount of noise that was introduced by the proposed technique to disturb the network and make it confused about the presence of the real event. Fig. 7 shows that even after the network is not overfitted, the test confusion matrix is still unable to distinguish the difference between real and fake events, which validate the high anonymity provided by the proposed technique.

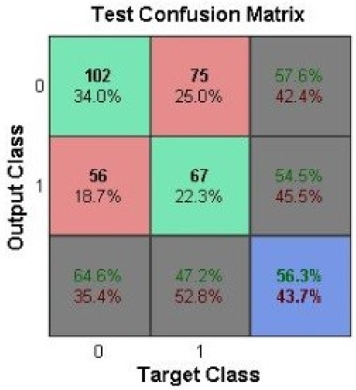


Figure 7: Test Confusion Matrix using 0.1 rate.

6.3 Steganography Model

The perfect system in terms of privacy is when $\boldsymbol{d(\alpha, \beta)}$ as described in equation 1 is equal to zero, which means the system is completely uncertain about the existence of the real event. Therefore it is obvious that the output of the anonymity equation for the proposed technique should be very close to 0. This confirms the high anonymity of our design. The confusion matrix (Fig. 8) created by the neural network is used to provide the false positives and false negatives, which are the values of $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ respectively. By using equation 1, $\boldsymbol{\alpha}$ is 0.499 and $\boldsymbol{\beta}$ is 0.486. Therefore the system anonymity $\boldsymbol{d(\alpha,\beta)}$ is 0.001 for the transmission rate of 0.2, which is very close to zero. This is another confirmation that the proposed technique provides a high level of anonymity because the adversary cannot tell if there is a real event or not.

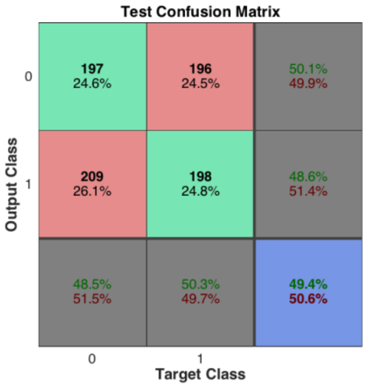


Figure 8: Test Confusion Matrix.

7 CONCLUSIONS

With the increasing importance of privacy and anonymity in many WSN applications, we developed a novel technique to reduce the overall transmission overhead of a network. The *EDAD* technique developed in this paper outperforms the previous techniques such as *DUD*, *DAD*, and *CAD* with respect to the overhead with an acceptable level of delay and delivery ratio. Visualization, neural network, and steganography models are developed to assess the anonymity of our approach. They provide a comprehensive analysis including time correlation, rate monitoring, and type of distribution unlike previous techniques such as *FitProbRate*, which only relies on the type of distribution. Results show that the *EDAD* technique provides a high level of anonymity under all three models, which provides a strong validation for the anonymity of the proposed work.

REFERENCES

[1] Pathan, A.-S.K., H.-W. Lee, and C.S. Hong. *Security in wireless sensor networks: issues and challenges.* in *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference.* 2006. IEEE.

[2] Dargie, W.W. and C. Poellabauer, *Fundamentals of wireless sensor networks: theory and practice.* 2010: John Wiley & Sons.

[3] Abuzneid, A.-s., T. Sobh, and M. Faezipour. *An enhanced communication protocol for anonymity and location privacy in WSN.* in *Wireless Communications and Networking Conference Workshops (WCNCW), 2015 IEEE.* 2015. IEEE.

[4] Spachos, P., D. Toumpakaris, and D. Hatzinakos. *Angle-based dynamic routing scheme for source location privacy in wireless sensor networks.* in *Vehicular Technology Conference (VTC Spring), 2014 IEEE 79th.* 2014. IEEE.

[5] Conti, M., J. Willemsen, and B. Crispo, *Providing Source Location Privacy in Wireless Sensor Networks: A Survey.* Communications Surveys & Tutorials, IEEE, 2013. **15**(3): p. 1238-1280.

[6] Mehta, K., D. Liu, and M. Wright, *Protecting Location Privacy in Sensor Networks against a Global Eavesdropper.* IEEE Transactions on Mobile Computing, 2012. **11**(2): p. 320-336.

[7] Gagneja, K.K. *Secure communication scheme for wireless sensor networks to maintain anonymity.* in *Computing, Networking and Communications (ICNC), 2015 International Conference on.* 2015. IEEE.

[8] Shao, M., et al. *Towards Statistically Strong Source Anonymity for Sensor Networks.* in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications.* 2008.

[9] Bradbury, M., M. Leeke, and A. Jhumka. *A dynamic fake source algorithm for source location privacy in wireless sensor networks.* in *Trustcom/BigDataSE/ISPA, 2015 IEEE.* 2015. IEEE.

[10] Chaudhari, M. and S. Dharawath. *Toward a statistical framework for source anonymity in sensor network using quantitative measures.* in *Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on.* 2015.

[11] Alomair, B., et al., *Toward a Statistical Framework for Source Anonymity in Sensor Networks.* Mobile Computing, IEEE Transactions on, 2013. **12**(2): p. 248-260.

[12] Yang, Y., et al., *Towards event source unobservability with minimum network traffic in sensor networks*, in *Proceedings of the first ACM conference on Wireless network security.* 2008, ACM: Alexandria, VA, USA. p. 77-88.

[13] Donnelly, R. and W.M. Kelley, *The humongous book of Statistics Problems.* 2009: Penguin.

[14] Bushang, A., A. Abuzneid, and A. Mahmood. *Source anonymity in WSNs against global adversary based on low rate fake injections.* in *Wireless Information Technology and Systems (ICWITS) and Applied Computational Electromagnetics (ACES), 2016 IEEE/ACES International Conference on.* 2016. IEEE.

[15] Bushnag, A., A. Abuzneid, and A. Mahmood, *Source Anonymity in WSNs against Global Adversary Utilizing Low Transmission Rates with Delay Constraints.* Sensors, 2016. **16**(7): p. 957.

[16] Katzenbeisser, S. and F. Petitcolas, *Information hiding techniques for steganography and digital watermarking.* 2000: Artech house.

[17] Huang, J., et al. *A source-location privacy protection strategy via pseudo normal distribution-based phantom routing in WSNs.* in *Proceedings of the 30th Annual ACM Symposium on Applied Computing.* 2015. ACM.

[18] Niu, X., et al., *An energy-efficient source-anonymity protocol in surveillance systems.* Personal and Ubiquitous Computing, 2016. **20**(5): p. 771-783.

[19] Yang, Y., et al., *Towards statistically strong source anonymity for sensor networks.* ACM Transactions on Sensor Networks (TOSN), 2013. **9**(3): p. 34.