Naive Bayes based Trust Management Model for Wireless Body Area Networks

Sm Rakibul Hasan Remu
Electrical & Electronic Eng.
Ahsanullah University of Science & Technology
Dhaka, Bangladesh
rakibremuaust@gmail.com

Md. Omar Faruque
Electrical & Electronic Eng.
Ahsanullah University of Science & Technology
Dhaka, Bangladesh
mohammadomarfaruque584@gmail.com

Rezowan Ferdous
Information & Communication Tech.
Bangladesh University of Professionals
Dhaka, Bangladesh
rezowan.7890@gmail.com

Md Murshedul Arifeen
Information & Communication Tech.
Bangladesh University of Professionals
Dhaka, Bangladesh
murshedularifeendipto@gmail.com

Sudman Sakib
Electrical & Electronic Eng.
Ahsanullah University of Science & Technology
Dhaka, Bangladesh
sakibsudman@gmail.com

S M Salim Reza
Faculty of Engineering and Built Environment
University Kebangsaan Malaysia
UKM, Selangor, Malaysia
salim4419@gmail.com

ABSTRACT

With the development of micro sensors, embedded technologies and wireless networking, Wireless Body Area Network (WBAN) is becoming a key emerging technology in healthcare to monitor and collect the biological data from the human body. Ensuring security of this network from compromised sensor nodes is a challenging task, as the traditional security mechanisms are not suitable and compatible with the lightweight body sensor nodes. In this paper, We have proposed a trust management model based on Naive Bayes classifier to classify a sensor node as trustworthy or malicious. Based on the classification the trustor node will choose a trustee node for the exchange of data. We have trained our proposed model in MATLAB and experimental results show that the proposed model can successfully classify a sensor node as a malicious or trusted.

CCS CONCEPTS

• **General and reference** → **General conference proceedings**; • **Security and privacy** → **Trusted computing**; • **Computer systems organization** → **Sensor networks**; • **Theory of computation** → *Bayesian analysis*; • **Computing methodologies** → *Machine learning*.

KEYWORDS

WBAN, Sensor Nodes, Trust Management, Naive Bayes

ACM Reference Format:
Sm Rakibul Hasan Remu, Md. Omar Faruque, Rezowan Ferdous, Md Murshedul Arifeen, Sudman Sakib, and S M Salim Reza. 2020. Naive Bayes based Trust Management Model for Wireless Body Area Networks. In *International Conference on Computing Advancements (ICCA 2020), January 10–12, 2020, Dhaka, Bangladesh.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3377049.3377084

ICCA 2020, January 10–12, 2020, Dhaka, Bangladesh

ACM ISBN 978-1-4503-7778-2/20/01…$15.00
https://doi.org/10.1145/3377049.3377084

1 INTRODUCTION

WBAN is a type of Wireless Sensor Network (WSN) that is deployed inside or outside of human body for different applications like blood pressure measurement, electroencephalography, blood bump, electrocardiogram, temperature measurement of the human body, location tracking etc. It is a special arrangement of sensor nodes that can collect biological and physiological data, forward these data to the coordinator nodes. Upon receiving these data, coordinator node sends these data to the personal server or medical database for medical emergency and inspection. Using the technology of WBAN, it is possible to reliably transfer patients data to emergency medical terminals and also mobility is supported seamlessly by the whole system [1].

Like other Sensor Networks such as WSN, WBAN suffers from energy limitation, memory limitation, processing power [2] which makes it challenging to implement robust cryptography algorithm for securing the WBAN network. Security issues including outsider attacks like eavesdropping, malicious attack and insider attacks by compromising sensor nodes can easily affect the data integrity, freshness and confidentiality [9]. Recent studies show that Trust Management can effectively mitigate insider attacks and it is a very promising and alternative solution to the cryptography mechanisms. Trust management allows for low power consumption and memory requirements and can mitigate insider attacks effectively [2].

We have modeled Trust management (TMM) based on Naive Bayes because of some features of Naive Bayes like its quicker ability to converge than other machine learning approach like logistic regression, dependability in spite of less amount of training data, linearly scaling by the number of predictors, dependable by both continuous and discrete data, lightweight feature and super simplicity [13]. Previously TMM in WBAN was based on few set of rules and factors that may affect the trust value and sometimes based on threshold. First one was time consuming and second one was

inefficient as threshold can vary based on different circumstances [14].So it is necessary to apply resource efficient trust model where sensor nodes can learn by themselves and can classify trusted and malicious nodes. Based on Naive Bayes, coordinator node can easily detect malicious or compromised nodes to make the whole network secured under any compromised condition.

Our Contribution In this paper we have proposed trust management mechanism based on Naive Bayes Classifier to eschew malicious or compromised node from the network.Based on the Trust Management model the coordinator node will judge the subordinate nodes whether they are malicious or not. Depending on the trust value,coordinator node[12] will eliminate or use any specific node in the network for data communication to sink node. The trust model dependency on Naive Bayes is simulated in MATLAB with a suitable output result.

2 LITERATURE REVIEW

To preserve privacy, symmetric cryptography keys are generated and distributed among sensor nodes. The authors in[8] explained how three layered Healthcare data flow can be protected. Different security schemes such as hardware encryption are used in WBAN architectures, on SNAP architecture Tiny Elliptic Curve Cryptography (ECC) security model is used, in case of Code Blue architecture on mica2 hardware ECC & TinySec security model has been used. The proposed system in [11] secured WBAN where the message authentication code (MAC) detects intruder and the decentralized IDS detects malicious devices. Data flow from biosensor nodes to BAN-head to health data center sensitive Data is secured through potential bio metric (heart rate variation) authentication system using decentralized rule based intrusion Detection system (IDS) at Ban-head and sink devices. For overcoming the challenges and enhancing the WBAN privacy issues two more techniques discussed in [10] are also efficient, Attribute Based Encryption (ABE) and ECC. These tools uses body's characteristics as parameter for key management which enhances the security but reduces the speed for transmission. In case of body area network attack-adaptable network can solve the trust issues the proposed BAN-Trust Scheme [7] can detect malicious nodes by observation and recommendation by other nodes. Limitations of this method is extensive experiments needs to be done. These limitations can be solved using machine learning technique. This recommendation information is shared between nodes to enhance trust management in WBAN [6] based on trust ratings but if the device is not previously interacted any other devices has issues in recommendations. Personal sensitive data in [5] often used for real time healthcare which needs emergency response for which ECC based encryption is used. The data from sensor stored as cipher text sink nodes know nothing only the relevant healthcare center and authorized doctor has the key and permission in the proposed model by author [3] so the model made the whole channel from sensor to doctor secured.Three main issues are described in [4] are loss, authentication and access control.

3 WBAN NETWORK SCENARIO

The network scenario of WBAN is classified by three tier architecture. The first tier consists of coordinator nodes and tiny sensor nodes. All tiny sensor nodes collect and transmit various physiological data to the coordinator node and coordinator node comprises a final data set for transmitting to second tier. Coordinator node can measure the trust value of every tiny sensor nodes. Second tier consists Personal Digital Assistant (PDA), Smartphone, Computer and finally the third tier consists Remote Servers, Medical Assistant and other entities that can analyze received data to provide helpful responses. An adversary can easily intercept the wireless channel and compromise any sensor node in the WBAN network.

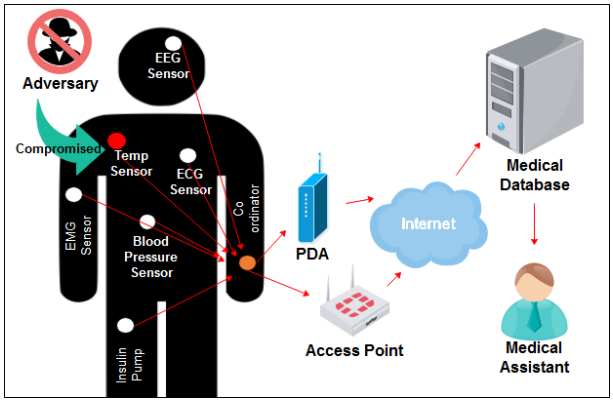

Figure 1: WBAN scenario where a coordinator node is collecting data and forwarding these data to the medical database

4 TRUST MANAGEMENT MODEL

This section demonstrates the proposed trust model based on Naive Bayes. A Naive Bayesian model has less complexity and is easy to build. It has no iterative parameter estimation which implies the easy feature and particularly useful behavior for very large data set of Naive Bayes. The Bayesian Theorem can be defined as,

$$p(x|y) = \frac{p(y|x) \times p(x)}{p(y)}$$

where, $p(x|y)$ = probability of class x given instance y, $p(y|x)$ = probability of instance y given class x, $p(x)$ = probability of occurrence of class x, $p(y)$ =probability of instance y occurring.

Naive Bayes classifier incurs the emancipation of all parameters. Bayesian theorem has one parameter, In case of many features or parameters, we can use all the features and simplify it with Naive Bayes classifier as,

$$p(y|x) = p(y_1|x) \times p(y_2|x) \times .... \times p(y_n|x)$$

In this paper, Naive Bayesian classifier has been applied for detecting malicious node in WBAN. The Packet Error Rate (PER) and Packet Loss Rate (PLR) have been considered as the features of Naive Bayes classifier. The malicious node intentionally drops packets or disseminate erroneous packet. From which we got inspired to include PLR and PER in the proposed trust model to evaluate the trustworthiness of a sensor node. Consider a node n under an evidence where PER=a and PLR=b and we want to calculate whether the node n is trustworthy or not. Where, a and b can be good, bad or medium. According to Naive Bayes, The trustworthiness can be predicted or classified as,

$$value = High : p(T = High) \times p(PER = a|T = High) \times p(PLR = b|T = High)$$
$$value = Low : p(T = Low) \times p(PER = a|T = Low) \times P(PLR = b|T = Low)$$
$$value = Moderate : p(T = Moderate) \times p(PER = a|T = Moderate) \times p(PLR = b| = Moderate)$$

where, T stands for trustworthiness. After calculation if predicted value = Low > predicted value = High > predicted value = Moderate, then node *n* is malicious. According to Naive Bayes Classifier we have classified the trustworthiness of the nodes as high, moderate and low. Then coordinator node will select the trustee node which has the high trust worthiness value. If there is no high trustworthiness then the coordinator node will select the trustee node which has moderate trustworthiness value. Coordinator node will always discard any trustee node whose trustworthiness is classified as low and that node will be considered as malicious node. Finally, the coordinator node will create alert for this situation. From figure 1 we can see that the node labeled as temperature sensor is compromised by an adversary, so its trust value will be classified as low and the coordinator node will make alert for this node and discard any packets it will receive from that compromised node.

Table 1: Sample predicted values of test data

PLR	PER	Predicted Classifications
0.14	0.24	M
0.15	0.32	M
0.48	0.27	L
0.47	0.11	M
0.35	0.17	M
0.21	0.48	L
0.01	0.14	H
0.08	0.36	M
0.29	0.43	L
0.11	0.31	M

Table 2: Specifications of training

ACCURACY	100%
Prediction Speed	720 obs/sec
Training time	23.751 sec

5 PERFORMANCE ANALYSIS

In this section, we will discuss about the performance of our proposed Naive Bayes based TMM. We have trained our Naive Bayes Based TMM in MATLAB. We have considered 80 random data sets to train our Naive Bayes model in MATLAB. Figure 2 demonstrates the classification of our trained data which implies the training has been done successfully where we wanted to influence the decay of trustworthiness to low with the increment of PER and PLR. After successful training we have taken few random data sets as input and got predicted classification as HIGH (H), LOW (L) and MODERATE (M). Figure 3 is the plot of accurate classification. Table 1 shows our specification of training the model and Table 2 shows speed, accuracy and time of training model.

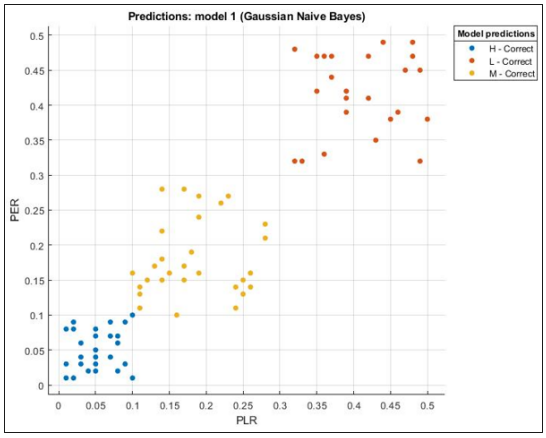

Figure 2: Classification of trust values after training the model

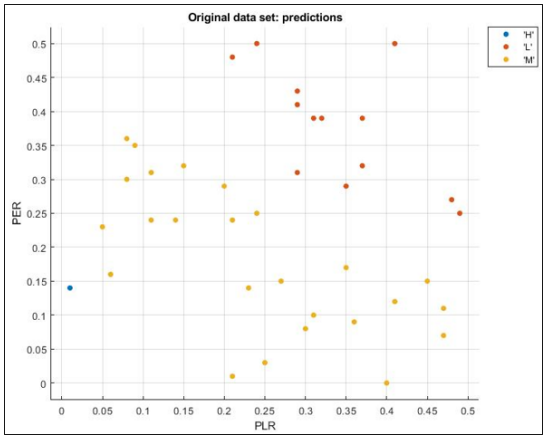

Figure 3: Classification of the test data by the proposed model

6 CONCLUSION

we have proposed TMM based on Naive Bayes classifier to detect malicious node in the network of WBAN. We have chosen WBAN as very few TMM progressed in WBAN. Here, Naive Bayes classifier has been shown as a trust evaluation model. We have described few progressive states in our model as node classification, detecting the malicious node, eliminating the malicious node. Coordinator node of the network always preserves the right to select or eliminate any tiny nodes. As we have represented our trained model and predicted model gained 100% accuracy which is indicator of seamless privacy of WBAN. In future, we will try to develop security of the coordinator node and we will increase the features like PER, PLR for decision taking.

REFERENCES

[1] Kemal Akkaya and Mohamed Younis. 2005. A survey on routing protocols for wireless sensor networks. *Ad hoc networks* 3, 3 (2005), 325–349.

[2] Md Murshedul Arifeen, Md Mustafizur Rahman, Kazi Abu Taher, Md Maynul Islam, M Shamim Kaiser, et al. 2019. ANFIS based Trust Management Model to Enhance Location Privacy in Underwater Wireless Sensor Networks. In *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*. IEEE, 1–6.

[3] M Gowtham and S Sobitha Ahila. 2017. Privacy enhanced data communication protocol for wireless body area network. In *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*. IEEE, 1–5.

[4] Ramesh Kumar and Rajeswari Mukesh. 2013. State of the art: Security in wireless body area networks. *International Journal of Computer Science & Engineering Technology (IJCSET) Vol* 4, 5 (2013), 622–630.

[5] Ming Li, Wenjing Lou, and Kui Ren. 2010. Data security and privacy in wireless body area networks. *IEEE Wireless communications* 17, 1 (2010), 51–58.

[6] Wenjia Li and Xianshu Zhu. 2014. Recommendation-based trust management in body area networks for mobile healthcare. In *2014 IEEE 11th International conference on mobile ad hoc and sensor systems*. IEEE, 515–516.

[7] Wenjia Li and Xianshu Zhu. 2016. BAN-trust: An attack-resilient malicious node detection scheme for body area networks. In *2016 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 1–5.

[8] Mohammed Mana, Mohammed Feham, and Boucif Amar Bensaber. 2011. Trust Key Management Scheme for Wireless Body Area Networks. *IJ Network Security* 12, 2 (2011), 75–83.

[9] Pejman Niksaz and Mashhad Branch. 2015. Wireless body area networks: attacks and countermeasures. *International Journal of scientific and engineering research* 6, 19 (2015), 565–568.

[10] Ibrahim Abdulai Sawaneh, Ibrahim Sankoh, and David Kanume Koroma. 2017. A survey on security issues and wearable sensors in wireless body area network for healthcare system. In *2017 14th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*. IEEE, 304–308.

[11] KM Sharmilee, Rajeswari Mukesh, A Damodaram, and V Subbiah Bharathi. 2008. Secure WBAN using rule-based IDS with biometrics and MAC authentication. In *HealthCom 2008-10th International Conference on e-health Networking, Applications and Services*. IEEE, 102–107.

[12] Weiwei Yuan, Donghai Guan, Sungyoung Lee, and Youngkoo Lee. 2006. A dynamic trust model based on naive bayes classifier for ubiquitous environments. In *International Conference on High Performance Computing and Communications*. Springer, 562–571.

[13] Harry Zhang. 2004. The optimality of naive Bayes. *AA* 1, 2 (2004), 3.

[14] Tong Zhang, Lisha Yan, and Yuan Yang. 2018. Trust evaluation method for clustered wireless sensor networks based on cloud model. *Wireless Networks* 24, 3 (2018), 777–797.