OPEN ACCESS
Saudi Journal of Engineering and Technology
Abbreviated Key Title: Saudi J Eng Technol
ISSN 2415-6272 (Print) |ISSN 2415-6264 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: http://scholarsmepub.com/sjet/

**Original Research Article**

# Designing a Fused Machine Learning Model for the Provision of Smart Health Care in MANETS

Kirori Gathuo Mindo*, Simon M. Karume, Moses M. Thiga

Kabarak University, Kenya

**DOI:**10.36348/SJET.2019.v04i09.005 | **Received:** 02.09.2019 | **Accepted:** 16.09.2019 | **Published:** 29.09.2019

***Corresponding author:** Kirori Gathuo Mindo

## Abstract

There is need to provide resilient security methodologies that do not require enormous computing resources. While entry prevention is the most viable disposition, it is not always possible to stop unauthorised access. Thus, it is critical to investigate the use of machine learning-based intrusion detection to buttress and provide sufficient security against DOS and other attacks in MANETs. Various anomaly-based intrusion detection systems employ varying techniques to identify anomalies in the context of diverse and valid variables. Most of these techniques, however, fail to capture and take account the physiognomies of MANETs. In the intervening time, usage of the internet of things in the provision of smart healthcare is expanding and the inherent risks snowballing. This study designed a model, which used a fusion of machine learning techniques through both simulation and a running prototype to achieve a more resilient intrusion detection system. The study was designed using functional decomposition methodology and implemented using PPDIO and evaluated on a MANET environment on both Linux NS 2 and further implemented on a network of Smart wearable devices and Raspberry Pi.

**Keywords**: MANET, Smart Healthcare, Intrusion Detection Systems, Machine Learning, Fused.



## INTRODUCTION

MANET networks have various protocols that perform various functions. An Ad Hoc On-Demand Distance Vector (AODV) routing protocol primarily supports mobile ad hoc networks. This protocol is responsible for establishing routes to destinations when requested and propagates unicast and multicast routing. Nokia, the University of California and the University of Cincinnati [1] jointly built this AODV protocol. The Temporally Ordered Routing Algorithm (TORA) is an algorithm that enables routing of data over Wireless and Mobile ad hoc networks. This algorithm reduces the number of required control messages within a network [2]. The Destination Sequenced Distance Vector (DSDV) is a distance-vector protocol that implores devices to update routing information intermittently. Devices on the network build a routing table that corresponds to ports, network and the distance to each of them. The protocol thus avoids the formation of routing loops that eat up resources on the network [3]. The optimised Link State Routing (OLSR) protocol is a link-state algorithm created to meet the requirements of a mobile ad-hoc network. The protocol minimises the message data by enabling devices to resend packets. The difference in this protocol is the ability to propagate, unlike classical link-state algorithms, temporary link-state information within the network [4].

### Statement of the Problem

DDOS attacks can conceal deteriorating health risks from discovery by both the patient and health specialist thus can lead to death, immobility, permanent or impaired disability. A patient's worsening condition might not be alerted to both the patient and health specialist as envisaged. Most IDS techniques fail to capture and take account of the characteristics of MANETs, which malicious attacks exploit. Existing intrusion detection methods are weak in identifying anomalous activity within a mobile ad-hoc wireless network.

## LITERATURE REVIEW

A security model is a symbolic representation of a particular security policy. It elucidates the requirements of the policy architects. A model is broken into a set of rules that should be adhered to within a computing system. A security model integrates various security requirements and delivers the obligatory arithmetic formulas, relationships, and domain structure

that must be adhered to to accomplish this security objective [5].

**Intrusion Detection Models for the MANET**

Intrusion Detection System is a security measure that can be installed on a network to prevent attacks from happening. The IDS allows network administrators to detect individuals trying to compromise the system so that they retrieve information from it. There are various activities that the administrators can detect in order to identify it. This includes security policies violation [6]. The IDS works best because it designed in a manner that enables it to detect the vulnerabilities on the system in which it is installed. For example, it can work on the basis of previous attacks that affected the network and work backwards to eliminate the chances of another similar attack. The IDS can detect attacks using various methods. For example, it can be done through signature-based detection. In these patterns are studied and compared to previous events or attacks and then identifies new threats. As a result, the system administrators can be able to identify new threats and other kinds of threats that the network is vulnerable to. An IDS is made of three basic components that include Network Intrusion Detection System (NIDS), Network Node Intrusion Detection System (NNIDS) and Host Intrusion Detection System. Each of these components plays a very vital role in securing networks [7].

The IDS technology is advancing on a daily basis and therefore organisations that acquire either of them should ensure that their system is up to date so that it can be able to handle even the most recent kinds of threats that can be launched on a given network. The IDS technology also is a reactive activity, not a proactive. This simply means that the IDS technology heavily relies on previous attack patterns. The technology cannot work independently. However, IDS technology is very important for any organisation that seeks to secure itself right from the network level [8].

Conceptual Framework

An anomaly-based intrusion detection model that fuses SVM and ANN is thus proposed to address the gap between bottlenecks in the two machine learning techniques. This is achieved by combining a variable matrix of the two machine learning techniques. A fusion of artificial neural networks and support vector machine data classifier was implemented. This enables proper monitoring and profiling traffic emanating from the WSN. The neural network is also supported through reinforcement learning so as to maximise the cumulative result. The network is then trained by introducing internet packet traces. The technical model will have the following components;

- A Data mapping separator
  - A Support Vector Machine.
- Anomaly Detection Engine
  - An Artificial Neural Network
- Alarm/Reporting Arm.

The Network collects all incoming/outgoing data transitioning through the interfaces. Packets are separated depending on interest and mapped accordingly to a higher dimensional feature space. This is fed into a Support Vector Machine that transforms a linearly non-separable problem into a linearly separable one. This is due to its strengths in data classification. Further, the classified data is fed into an artificial neural network that performs pattern recognition tasks. The ANN makes us of modified probabilistic radial basis function. Data packets with the anomalous symbol are thereafter passed into the anomaly detection engine. If the data is positive, an alarm is raised, and a particular anomaly is reported.

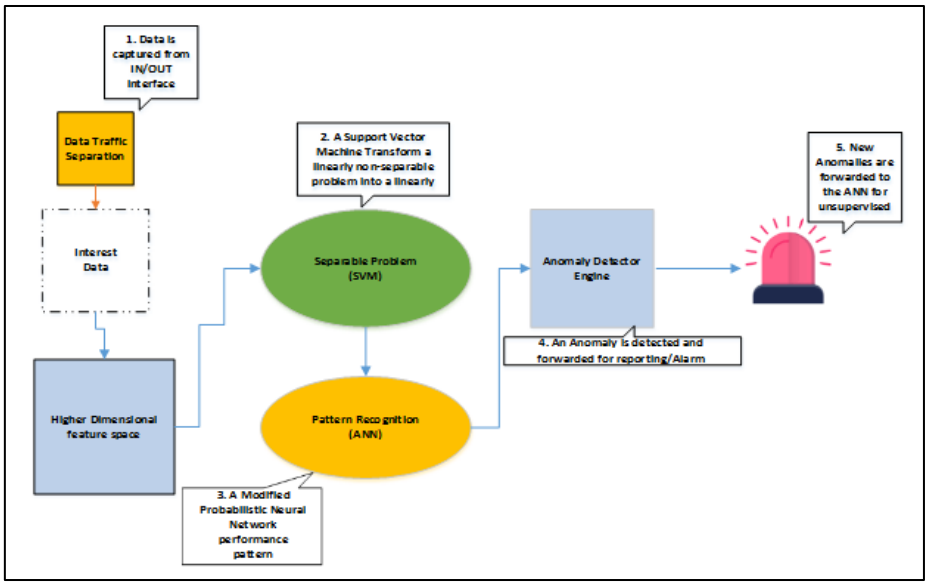


**Fig-1: Conceptual Framework**

# METHODOLOGY

## Design of a MANET ABID Model for Smart Healthcare

### *PPDIO methodology Research Design for Model Design*

This study adopted a mixed-methods approach research methodology to design, develop, implement and test the model for a fused anomalous intrusion detection system. The two major methodologies used were the Prepare, Plan, Design, Implement, Operate, and Optimise (PPDIOO) and the Proof of Concept Methodology.

The PPDIO methodology is essential for wireless sensor networks that are inherently complex and difficult to manage. This methodology defines a continuous top-down life cycle of services that supports dynamically evolving networks. It follows six phases, each that describes the continuous life cycle of MANET network services that are essential for the interconnection and propagation of a network [11. The model experientially simulated a computational immunology status of an anomalous intrusion identification, isolation and detection. This methodology is idyllic since it lowers cost of ownership, increases the MANET network availability and improves business agility. Ultimately, the methodology accelerates MANET devices access and integration with application layer services.

# PROTOTYPE DEVELOPMENT AND RESULTS

## Design of A MANET Anomaly-based Intrusion Detection Model for Smart Health care

This section presents the results of the objective of the study, which set out to design a fused machine learning intrusion detection model for the provision of smart health care in MANETS. The Design aspect of the Model was implemented in various ways, as shown in the following steps, below. The design of the fused MANET anomaly-based intrusion detection model for the provision of Smart Healthcare undertook this design approach so as to accomplish three critical achievements;

- Logical Topology- Design implemented as a model using the functional decomposition methodology.
- Achieve a Logical Topology to describe the organisation and connectivity of smart devices to the smart IDS system within the MANET. How these devices receive/send data and how the IDS audit the data being propagated in the MANET ecosystem. This does not describe how the devices physically interconnect; however, this logical topology is considered isomorphic to the physical topology
- Model Logical Events - Design implemented as a Finite State Machine (FSM) using PPDIO methodology.
- Model the various Logical Events that describe normal and anomalous activity within a MANET.
- Network Connectivity - This implemented as a model using PPDIO methodology and implemented on Linux NS2 and as a live experiment as well.
- Achieve a physical network topology describing how the devices physically interconnect; however, this physical topology is considered isomorphic to the logical topology.

### Design of Logical Topology

The design of this logical topology was achieved using functional decomposition. Functional decomposition is a methodology of systems analysis that separates a complex entity to describe the separate contributing components. Functional decomposition enables understanding and organisation of complex entities, which are used to help solve problems and thus help to develop business operations, computer systems and machine learning among various other use cases [9]. The methodology was deemed best since the research comprised of fusion of two discrete individual processes and techniques. This enabled a flowing description of the functional relationship between the various constituent components and integration of separable logical processes herein compressed into a representation of the global IDS.

### The steps followed in Functional Decomposition are

- Find the basic function – This describes the basic task a device or process must succeed at achieving.
- List the essential sub-functions – This describes the various sub-functions, which are key to the success of the basic function.
- List the next tier of sub-functions - This describes the sub-functions, which serve the upper-level sub-functions.
- Inspect the diagram – Enables the researcher to inspect and identify functions that might have been omitted and add them to the diagram.

### The two constituent components were

- A Data mapping separator using a Support Vector Machine.
- Anomaly Detection Engine using an Artificial Neural Network

### Design of a Data Mapping Separator using Support Vector Machines

A review of Support Vector Machine algorithms for data classifiers was done. This involved identifying the right and relevant interest data which is consequently captured, segregated and analysed. In the proposed model, as shown in Figure 2 below, a node in the mobile ad-hoc network participates in MANET by sending or receiving packets via Bluetooth.

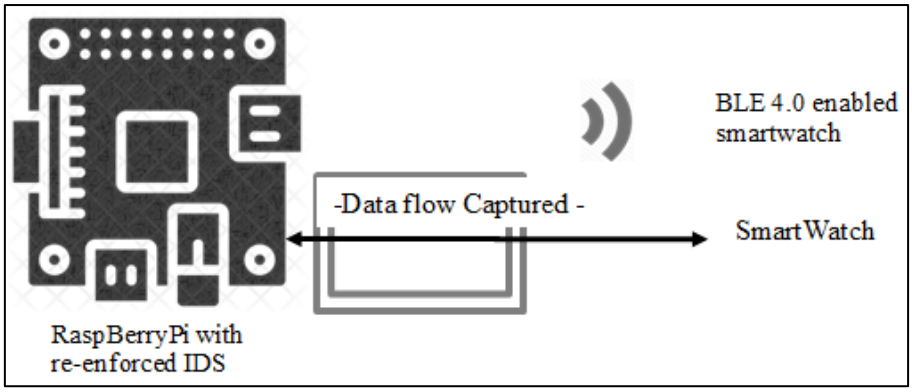


**Fig-2: The Logical Topology for Data Capture from the smartwatch Bluetooth device**

Once the devices are connected, an instance of a Linear SVM classifier is initiated, as shown in Figure 3 below. Interest data is separated from all the data available within the MANET. This is classified into no-interest, interest and high-interest data as shown in Table 1 below;

*Table-1: Categorisation of packet flow to interest data*

| No. | No-Interest | Interest | High Interest |
|---|---|---|---|
| **1.** | DSR | BTHCI_ACL | TCP |
| **2.** | AODV | BTHCI_CMD | UDP |
| **3.** | TORA / LMR | BTHCI_EVT | |

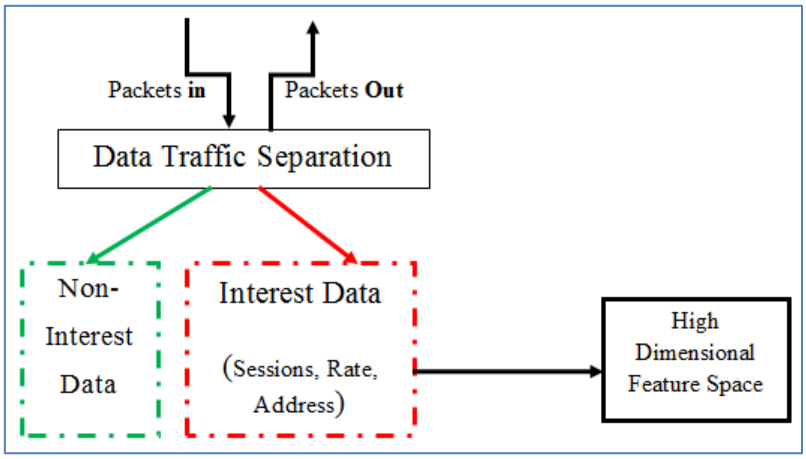


**Fig-3: Data Classifier Model**

Figure 3 shows the Data Separator Sub-Model, which was designed using the functional decomposition methodology and implemented as a running experiment using Support vector Machine data classifier algorithms. The model in figure 2 monitors packets flowing into and out of the network and separates them accordingly. Packets, which are of interest to the IDS, are forwarded for analysis. The SVM algorithm generates a hyper-plane, which segregates the interest data according to behaviour, rate and type separating the two classes correctly. The trained a Linear SVM classifier compares the two vectors separated by the decision boundary or hyper-plane with the two nearest neighbour packets data points (D+ and D-). The results of SVM are then fed into an Artificial Neural Network algorithm.

**Design of the Anomaly Detection Engine using Artificial Neural Networks**

The design of the Anomaly Detection Engine using Artificial Neural Networks was also achieved through functional decomposition methodology. This was a result of delinking the various components from the overall conceptual framework, to identify the sub-model designs. Figure 4 below shows the interaction between SVM and ANN engines. This is the fusion stage of the fused Anomaly detection model.

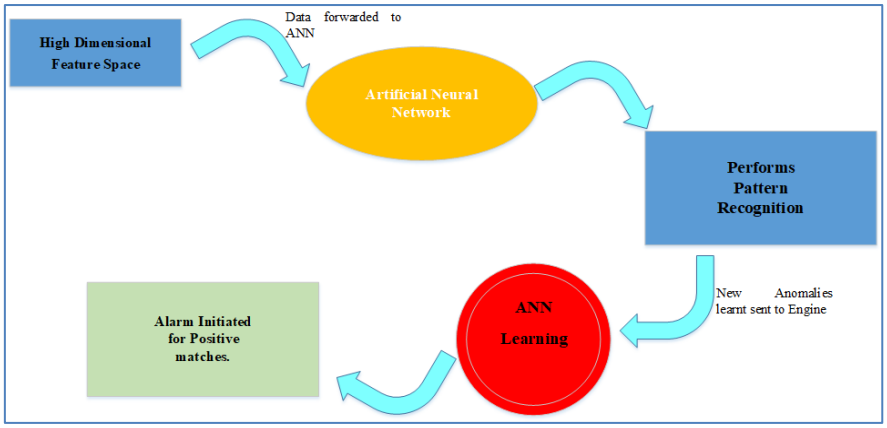


**Fig-4: SVM into ANN integration**

Data classified by the SVM algorithm is fed into the Artificial Neural Network that performs pattern recognition tasks. The ANN applies modified probabilistic radial basis function (PRBF) to perform pattern recognition tasks. This approach is normally applied on various test problems, which have multiple uncertain parameters, to improve and harness some insights. Combinations of different radial basis functions and sampling techniques are used to study the performance of different combinations. Data packets with the anomalous symbol are thereafter passed into the anomaly detection engine. If the data is positive, an alarm is raised, and a particular anomaly is reported. The Alarm function can also feed forward into the artificial neural network for continuous learning.

**Design of a Finite State Machine to describe Normal and Anomalous Events within a MANETs**

This design section was implemented as a Finite State Machine (FSM) using PPDIO methodology. FSM is an artificial intelligence technique that allows predictability with a given set of inputs and a known current state; therefore, state transitions can be easily predicted and thus enable for easy testing. FSM also enable determination of reachability of a state thus when these states are represented in an abstract form; it is insentient clear whether one state can be arrived at from another state, and what is required to arrive the state [10].

**Design of a State Diagrams for MANET propagation activities**

State diagrams are a visual representation of the various states, inputs and outputs of a finite state machine. The state diagrams design was produced because of state transition tables, which describe the outright logic for every state and resulting state once the input is received to the automaton. On the basis of the transition table in (a) above that presents the various data propagation scenarios, an abstracted visual connectivity design for the prototype MANET network was designed so as to exhibit connectivity between two nodes. The Transition figure below abstracts the role of nodes and routers. MANET nodes are mobile and are most commonly connected dynamically in an arbitrary fashion. These nodes within MANET networks behave as both nodes and as routers, which are responsible for route discovery and route maintenance of routes.

**Finite State Diagram Logic for Normal Activity within MANETs**

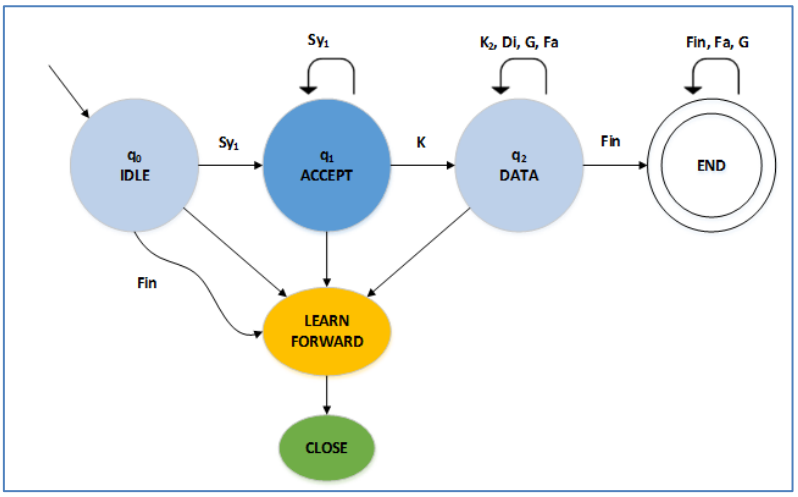


**Fig-5: FSM for Normal Transition Activity in MANETs**

Figure 5 above is an abstract MANET machine where nodes transition from a sleep or idle mode and initiate data transfer in various ways depending on the type of data – control data, normal data encapsulated as either TCP or UDP type. The transitions regarded as normal transitions with any deviation marked as anomalous (X) as in the state assignment step in (d) below.

**Finite State Diagram Logic for TCP activity**

A spread algorithm was used to create a Finite State Machine for abstracting TCP sessions in MANETs. The machine includes formal notations in TCP connections where MANETS are only established by satisfying the following;

- Packets are exchanged over the same TCP port;
- The source and destination IP addresses are commensurately matched;
- The sequence numbers are in sync;
- And, acknowledgement numbers match correctly. The FSM design below thus takes the above into consideration, and the following case scenarios were set, as shown in the Transition Figure 6 below.

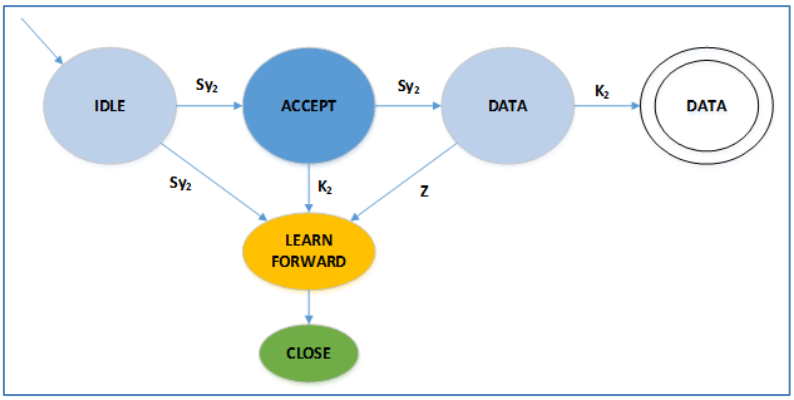


**Fig-6: Shows the Normal and Anomalous FSM for TCP sessions in MANETS.**

TCP in MANET follows the same transition to achieve the TCP 3-Way Handshake. MANET devices have a sleep or idle state from where all sessions originate. The anomalous transitions are indicated with an (X) as in the state assignment step in (d) below.

**State Minimisation of Finite State Machines**

State minimisation is the process of reducing or transformation of a given FSM into an equivalent but a smaller machine with n redundant states. This step can be optional for FSM that do not have redundant or indistinguishable states. The goal of this step is to identify and remove redundant states if any.

The FSM for UDP voluminous amplification in UDP exhibited various indistinguishable states and as well as amplification of Denial of Sleep. Since the devices amplify every iteration PR with a commensurate PF, as shown in Figure 9 below, a minimised FSM for this is presented, as shown in figure 7 below.

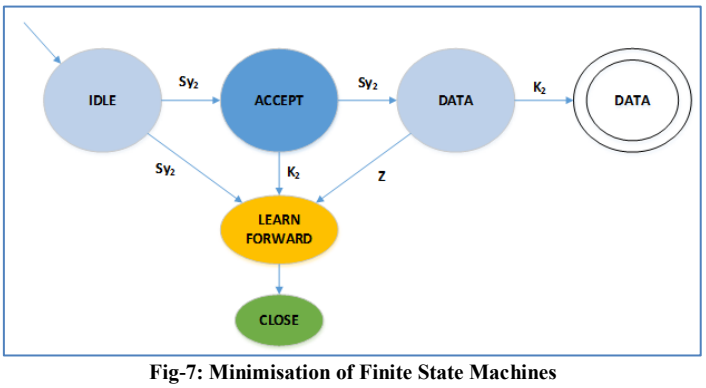


**Fig-7: Minimisation of Finite State Machines**

**State Assignment for acceptable and anomalous inputs**

State assignment is the process of using state transition variables to express specific states and expound how the values of these state variables are arrived at. Table 3 below enumerates the state transition variables that identify invalid inputs within a TCP activity showing during normal and anomalous data exchange.

**Table-2: State transition variables that identify invalid inputs within a TCP session**

| Transition | q0 | q1 | q2 | q3 | LF | Close |
|---|---|---|---|---|---|---|
| State | O | Sy1 | X | X | X | O |
| | Sy1 | Sy1 | K2 | Sy1 | X | G |
| | K2 | K2 | K2 | D | X | G |
| | D | X | X | D | X | G |
| | Fin | X | X | X | Close | G |
| | G | Sy1 | X | X | X | G |
| | An | - | - | - | - | G |

The following transitions are thereby flagged as anomalous by the function notation
!normal Transition/State = X
For State O, X = Sy1 for q1,q2,q3
For State Sy1, X = q3
For State K2, X = q3
For State D, X = q0, q1, q3
For State Fin, X = q0, q1, q2, q3
For State G q1, q2, q3

**Design of the Integrated Network Connectivity within a MANET**

This Network Connectivity Model was designed using Prepare, Plan, Design, and Implement, Operate, and Optimise (PPDIO) methodology. This was to be later implemented on Linux NS2 and as a live experiment. This section achieved a physical network topology describing how the devices physically interconnect; however, this physical topology is considered isomorphic to the logical topology.

The objective of this network connectivity design was;

- Show the interrelation between the physical network and logical topology
- Show the interaction between data handlers and the fused IDS engine

The design of the network connectivity is presented in Figure 8 that follows below;

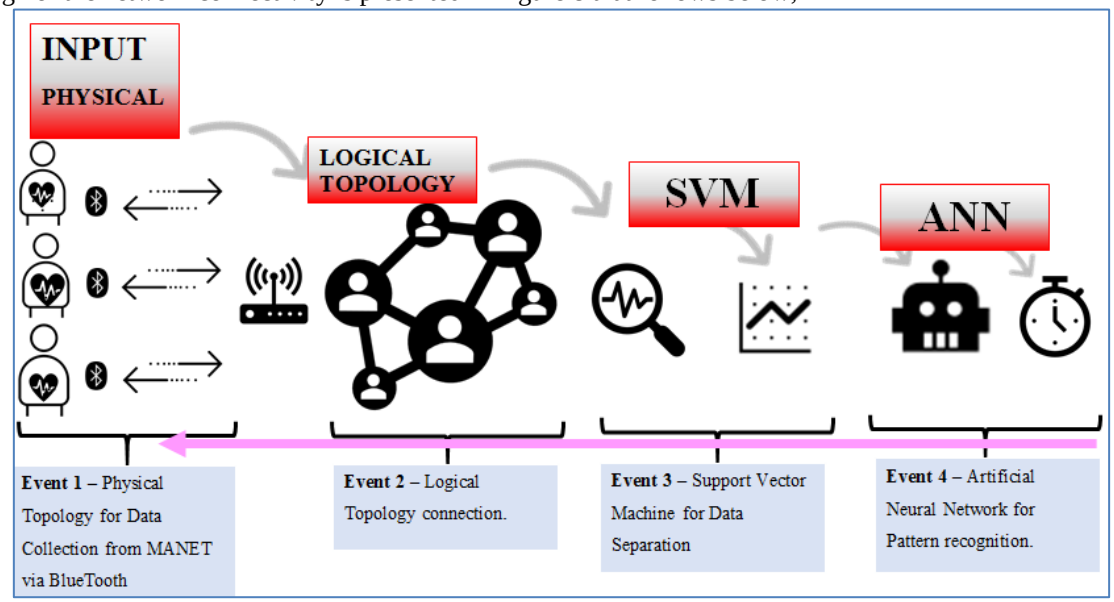


**Fig-8: Model Design for the Fused Machine Learning Intrusion Detection Model for the Provision of Smart Health Care in MANETS**

**The Model Design for the Fused Machine Learning Intrusion Detection Model for the Provision of Smart Health Care in MANETS**

The first event 1 presents the physical topology of the MANET, whereby Bluetooth enabled smartwatch captures raw user data and forwards the same to the MANET ecosystem. For this particular research, the envisaged data to be collected is the patients' blood pressure, and the hardware devices are suited for the same. The physical connection is deemed to be Blue Tooth 4.0 and above. These devices are deemed to be mobile and exhibit the characteristics discussed.

Event 2 presents the logical topology provided through ad-hoc connectivity service set. MANET Devices connect randomly and dynamically since they are free to roam dynamically changing the network topology frequently. Each node is expected to forward traffic unrelated to its own use, and thus must behave as a router. The MANET is required to consistently keep network routing information to properly forward packets correctly and efficiently. This MANETs topology can either be standalone or can also be connected to the Internet.

Event 3 above presents the support vector machine engine that is responsible for capturing all the data propagated in the MANET. The SVM thereafter identifies interest data and segregates the data into various interest groupings. The data is segregated into interest and non-interest data. Interest data is regarded as that whose input is likely to lead to an anomalous state.

The ANN function is to perform pattern recognition. Interest data received from the SVM is matched against rules described by the FSM to check whether its inputs or events are considered unacceptable, thus anomalous. If the ANN finds events or input which match those patterns considered anomalous, the alarm is raised and these events are recorded and fed forward into the smart devices.

## CONCLUSION

The design was premised on the ability of the MANET to identify intrusions by taking cognisance of unfamiliar device addresses, not permitting TCP sessions that are initiated by devices outside its network to get into fruition and identify scenarios that cause high resource usage in COU, Ram and bandwidth within the ecosystem as well. To achieve this, three designs were resultant. A logical topology design, which was a refined conceptual framework using functional decomposition methodology, to present the logical interconnection. A model of logical events, which described the various MANET activities, considered as normal and those considered anomalous.

## REFERENCES


1. El Hassani, A. A., El Kalam, A. A., Bouhoula, A., Abassi, R., & Ouahman, A. A. (2015). Integrity-OrBAC: A new model to preserve critical infrastructures integrity. *International Journal of Information Security*, *14*(4), 367-385.
2. Patel, N. J. K., & Tripathi, K. (2018). Trust value-based algorithm to identify and defend grey hole and blackhole attack present in MANET using Clustering Method. *International Journal of Scientific Research in Science, Engineering and Technology*, *4*(4), 281-287.
3. Singh, G., & Dhir, V. (2018). Performance analysis of Adhoc on-demand distance vector (AODV) and destination sequence routing (DSR) protocols in mobile Adhoc networks (MANET). *Global Journal of Computer Science and Technology*: *E-Network, Web & Security*, *18*(2), 21-28.
4. Poularakis, K., Iosifidis, G., & Tassiulas, L. (2018). SDN-Enabled Tactical Ad Hoc Networks: Extending Programmable Control to the Edge. *IEEE Communications Magazine*, *56*, 132-138.
5. Almorsy, M., Grundy, J., & Muller, I. (2010). An analysis of the cloud computing security problem. In *Proceedings of the 2010 Asia Pacific Cloud Workshop. Australia, APSEC2010*.
6. Chaudhary, A., & Shrimal, G. (2019). *Intrusion Detection System based on genetic Algorithm for detection of distribution denial of service attacks in MANETs*. Retrieved from SSRN 3351807.
7. Benkhelifa, E., Welsh, T., & Hamouda, W. (2018). A critical review of practices and challenges in Intrusion Detection Systems for IoT: Toward universal and resilient systems. *IEEE Communications Surveys & Tutorials*, *20*(4), 3496-3509.
8. Taher, K. A., Jisan, B. M. Y., & Rahman, M. M. (2019). Network intrusion detection using supervised machine learning technique with feature selection. In: *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)* (pp. 643-646). IEEE.
9. Harris, G., & Davies, H. (2019). Simulating information retrieval systems and functional decomposition. *International Journal of Software Systems Research and Methodology*, *4*(1).
10. Groz, R., Simao, A., Bremond, N., & Oriat, C. (2018, May). Revisiting AI and testing methods to infer FSM models of black-box systems. In: *2018 IEEE/ACM 13th International Workshop on Automation of Software Test (AST)*. IEEE. 16-19
11. Evans, D. (2011). *The Internet of Things: How the next evolution of the internet is changing everything*. San Jose, CA: Cisco Internet Bussiness Solutions Group.