Computers, Materials & Continua
DOI:10.32604/cmc.2021.016076
Article

Tech Science Press

A Reliable and Scalable Internet of Military Things Architecture

Omar Said[1,3] **and Amr Tolba**[2,3,*]

[1]Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif, 21944, Saudi Arabia
[2]Department of Computer Science, Community College, King Saud University, Riyadh, 11437, Saudi Arabia
[3]Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin Elkoum, 32511, Egypt
[*]Corresponding Author: Amr Tolba. Email: atolba@ksu.edu.sa
Received: 22 December 2020; Accepted: 23 January 2021

Abstract: Recently, Internet of Things (IoT) technology has provided logistics services to many disciplines such as agriculture, industry, and medicine. Thus, it has become one of the most important scientific research fields. Applying IoT to military domain has many challenges such as fault tolerance and QoS. In this paper, IoT technology is applied on the military field to create an Internet of Military Things (IoMT) system. Here, the architecture of the aforementioned IoMT system is proposed. This architecture consists of four main layers: Communication, information, application, and decision support. These layers provided a fault tolerant coverage communication system for IoMT things. Moreover, it implemented data reduction methods such as filtering, compression, abstraction, and data prioritization queuing system to guarantee QoS for the transmitted data. Furthermore, it used decision support technology and IoMT application unification ideas. Finally, to evaluate the IoMT system, an intensive simulation environment is constructed using the network simulation package, NS3. The simulation results proved that the proposed IoMT system outperformed the traditional military system with regard to the performance metrics, packet loss, end-to-end delay, throughput, energy consumption ratio, and data reduction rate.

Keywords: Internet of things; internet of military things; simulation; military; battlefield

1 Introduction

The term *Internet of Things (IoT)* can be defined as communication between huge numbers of things all over the world [1,2]. Recently, the term IoT has been used in many research fields such as mobile ad hoc networks, cloud computing, cyber-physical systems, big data analytics, etc. Additionally, IoT technology has improved the services which are introduced in many fields such as medical, commercial, traffic, security, and other applications [3,4]. Therefore, research in the IoT field has devoted considerable attention [5–7]. Because of the relationship between industrial,

commercial, and military fields, applications of IoT technology in the military field have increased in number [8–10].

The modern war has become mainly information-based. Recently, United States forces have become dependent upon use of the central information network in all war strategies. This is considered a recent concept in warfare's world compared with traditional plans [11]. Additionally, real-time information sharing between military sectors is one of the most important things involved in managing wars, especially if these types of information are critical and if timely knowledge of this information will lead to the resolution of many critical situations [12]. Thus, communication between war elements such as weapons, applications, soldiers, and other elements to become one information network has become an important research [13]. The main target of the IoMT is to provide better efficiency in the battlefield.

There are many challenges in the IoMT field due to its special nature. The main challenge is presented by the communication between different types of weapons in addition to other things such as soldiers. This type of communication should consider the critical battlefield situations that may require real-time decisions. Moreover, the fault tolerance aspect is an important communication issue and should be considered when the IoMT system architecture is designed. Therefore, in case of failure in a communication strategy between groups of military things, an alternative manner of communication should be ready to complete the communication target. The second challenge which should be considered concerns scalability. In the battlefield, the number of interaction processes occurring between huge numbers of entities increases with time. Therefore, the IoMT system architecture should consider the joining and leaving of billions of things. Nonetheless, traditional scalability protocols cannot be applied with this type of environment because its resources may be limited (i.e., bottlenecks). The third challenge presented by the IoMT is related to energy consumption. There are many things in the IoMT environment which are energy-based. Hence, in the case of full capacity consumption by a battlefield thing, this thing will become useless. This may raise a major problem, especially if this thing has high importance. The fourth challenge concerns interoperability. This challenge can be simply defined in the IoMT by different applications which will be used in the battlefield. The fifth challenge is that of ensuring *quality of service (QoS)*, which can be defined as the ability to provide a service required for data to be transmitted in a real-time manner.

The main contributions of this paper:

- We develop a scalable IoMT system architecture.
- We Propose a fault tolerant coverage communication system for IoMT things.
- We implement data reduction methods such as filtering, compression, and abstraction in addition to data prioritization in the IoMT system to guarantee QoS.
- Furthermore, we use decision support technology and IoMT application unification ideas.
- Finally, we construct a simulation environment to test the performance of the proposed IoMT system and discuss the simulation results.

The reset of the paper is organized as follows: The "related works" are discussed in Section 2, the proposed IoMT system architecture is presented in Section 3, the construction of the simulation environment is demonstrated and the results are discussed in Section 4, and the paper is concluded in Section 5.

2 Related Works

Most of the aforementioned researchers did not attempt to apply or simulate what they had demonstrated. Yushi et al. [14] introduced IoMT system conception and architecture as well as an application assumption to validate the proposed IoMT modes. The main weakness in this research trail is that there is no simulation or implementation for the demonstrated modes. The system architecture can be simplified by combining a set of layers. Moreover, management and security processes should be distributed over the whole set of architectural layers. Chudzikiewicz et al. [15] introduced a fault tolerance technique to the IoMT system. A simple implementation of the IoMT showed few results. The proposed implementation scenario is too simple, so it cannot reflect the real nature of the IoMT environment. Thus, the implementation results are considered inaccurate. Głowacka et al. [16] presented a cognitive mechanism to make the IoT-based military system aware of threats. Once again, the main weakness of this mechanism was that the simulation environment which was used to test the proposed mechanism did not reflect the real nature of the IoMT. Kott et al. [17] presented a survey about the Internet of Butterflied Things (IoBT). Management, communication, deception, and adversarial perspectives were also introduced. This research presented only a theoretical meaning. Tortonesi et al. [18] presented a survey about the IoT which comprised its information management and communication challenges. Additionally, this survey demonstrated specific military operations built on the IoT concept. The simulation infrastructure which was used to measure the performance of the proposed military operations is too trivial to be considered an IoMT environment. Pradhan et al. [19] proposed an approach that used commercial off-the-shelf (COTS) sensors for data gathering and surveillance. They also highlighted usage of IoT devices for military purposes. However, no implementation or simulation of the authors' claims was considered. Dyk et al. [20] presented an ontological technique to both evaluate the information network and consider the butterflied soldier's health. Moreover, a simulation environment was introduced to test the proposed technique. This research used a simulation package called SenseSim, which is related only to WSN. (The IoT comprises not only WSN but also comprises other things from RFID networks, mobile ad hoc networks, etc.) Therefore, the proposed simulation results are considered inaccurate. Jalaian et al. [21] presented a proof for using the IoT concept in military applications. It presented an architecture which utilized a long-range low-power wide-area network (LoRaWAN). This research is considered the nucleus of the idea of using the IoT for military purposes. However, LoRaWAN is simple and based only on the sensors and embedded micro-controllers equipped with LoRaWAN-compatible radio. This is contrary to the nature of the IoT technology. Johnsen et al. presented a medium-sized smart city scenario. This scenario described a simple information management system that may be useful in Situational Awareness (SA) issues [22]. Additionally, a military application perspective has been introduced in the smart city scenario to be applied in the future.

3 The Proposed IoMT System Architecture

The IoMT system comprises a group of military things which should be well-organized in the battlefield. These things, such as drones, operating bases, ships, tanks, soldiers, and planes, should be communicated in a cohesive network. Situational awareness, response time, and risk assessment are all increased in the IoMT network. Furthermore, the IoMT environment should involve a complete awareness of pervasive computing, pervasive management, pervasive sensing, and pervasive communication. Furthermore, the IoMT may lead to an extraordinary scale of data produced by the network things such as sensors. Moreover, the computations which are required

in this type of network are massive, and the results of these computations should be achieved accurately in real time. Therefore, the IoMT system architecture should consider above notes.

Thus, the proposed architecture consists of four layers: Communication, information, application, and decision support layers (see Fig. 1). The communication layer is concerned with how the things can communicate with each other in one large network. The information layer is concerned with the collection, management, and analysis of military data. The application layer comprises the application(s) that control the differently-communicated military systems. Finally, the decision support layer is concerned with the decision support system that helps the war managers make accurate, real-time decisions. Each layer will be discussed in depth below.

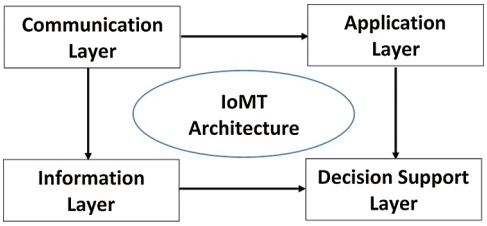

Figure 1: Simple view of the proposed IoMT architecture

3.1 The Communication Layer

The IoMT system can be considered a special example of the IoT. Hence, the IoMT environment is somewhat similar to the IoT environment with minor differences in types of things, communication manners, etc. In accordance with this idea, the IoMT environment can be defined as a group of different networks communicating with each other using the Internet. These networks should comprise active and passive things that can be found in military missions. The main networks which should be constructed in the IoMT system include wireless sensor (WSN), radio-frequency identification (RFID), mobile ad hoc (MANET), satellite, and high-altitude platform (HAP) networks. The WSN is represented in the IoMT system due to its importance in many military issues. The WSN assists war operations by rapidly collecting and delivering precarious data. Then, this data is sent to the most suitable person to make a correct decision in real time. Therefore, the main target of the WSN is to monitor and track the movements of enemy soldiers and other enemy things, in addition to coordinating its own military activities. Sensors can be distributed over long distances and cover large areas. These sensors communicate using base stations which control their behaviors. RFID network is represented in the IoMT environment due to its importance in the military field. One of most important issues in the army is that most of its things should be tagged. Using RFID in the battlefield provides a tracking system with superintendence for soldiers, cargo, small weapons, airplanes, projectiles, missiles, etc. For example, periodically scanning the medical case and efficiency of each person is a very important issue in the wars. MANET representation in the IoMT system is also an important issue because it can be used to facilitate the communications of soldiers, weapons, vehicles, etc. MANET has many ad hoc military applications, such as a network installed between airplanes and ground stations or a network between ships. The requirements of each ad hoc network are determined depending on the military mission type. Moreover, the ad hoc devices which are used in military applications are equipped with routing scenarios such that data can be forwarded automatically using best routing paths. It is common logic that the IoT relies on Internet technology to facilitate communication. Unfortunately, Internet technology may not be available in some battle locations.

Therefore, finding alternative communication technologies is very important. This is why the HAP network is used in the coverage target. The military things are distributed over large areas, so they should be covered in a reliable manner to guarantee communication efficiency. The HAP network can be used as a second communication strategy option in addition to the Internet. The HAP network can be found at limited heights; therefore, it could be an easy target for the enemy and its failure probability may be high. In cases of HAP network failure, the communication system will face big problems which may affect the military mission. Therefore, a satellite network should be constructed to cover the failed HAP network, and to cover the military things which may be not covered by HAP networks or the Internet (see Fig. 2). The communication challenge between different networks is resolved simply using a header recovery technique. In this technique, a translator which encapsulates each packet with the header of the destination node should be added between each two networks. The new header makes the packet understandable; this can be achieved by the system routers (see Fig. 3).

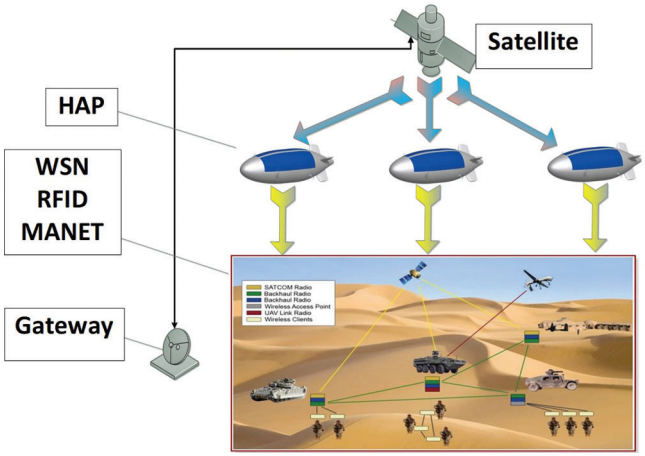

Figure 2: The communicated networks (part from this figure is taken from [23])

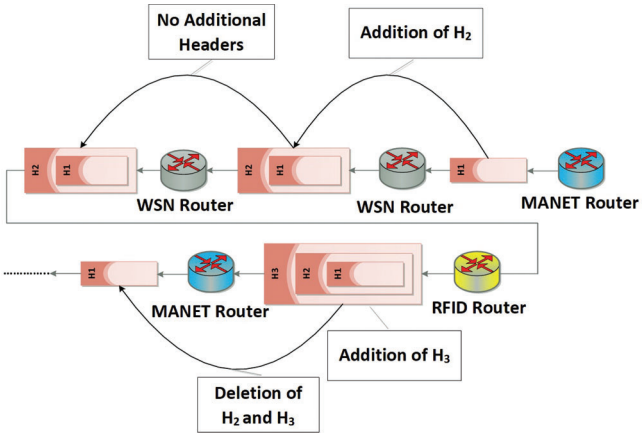

Figure 3: The header translation process

3.2 The Information Layer

This layer is very important because it represents the core of the IoMT system architecture. The information collected by military things such as RFID, sensors, etc. should be transmitted, stored, and analyzed in a secure, precious, real-time manner. The first function of this layer is the organization and storage of gathered information after this information has been processed. The processing of IoMT system data is considered a challenging issue due to the terabytes of data that can be gathered within a short period. Therefore, this data should be minimized to an extent that will not compromise quality. Additionally, the special requirements of IoMT, such as real-time decisions, cannot be neglected. In the IoMT system architecture, data processing comprises four steps: Prioritization, filtering, compression, and abstraction. The prioritization process is clarified below. Data filtering, data compression, and data abstraction techniques are stated in Sub-section 4.1.

The prioritization step involves handling data at different priority levels. Each piece of data collected has a certain level of importance for the war managers (i.e., army generals). Therefore, data should be organized into a number of priority levels such that the high priority data will be handled and sent first in cases of IoMT system starvation. A queuing system is used to achieve this prioritization step. Due to the huge number of IoMT system data classifications, a six-queue system is used. Hence, the IoMT system data will be classified into six different classes. The first class represents the most important IoMT system data; the second class represents the less important data, and so on. The classification process will be accomplished dynamically, so the data in each class may change depending on the nature of the war mission. To achieve this step practically, next router generations should have the ability to classify IoMT system data. Fig. 4 clarifies the prioritization process.

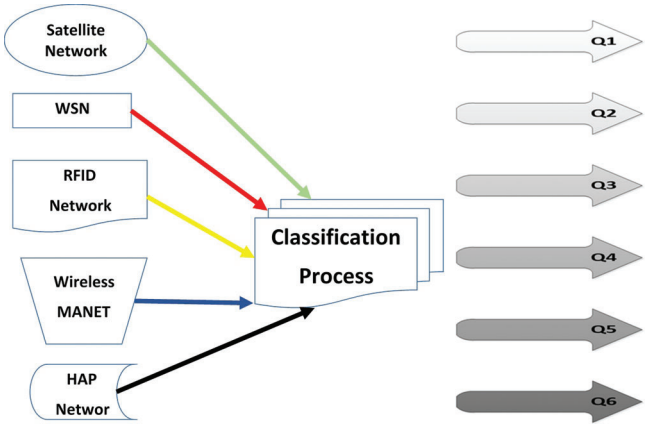

Figure 4: Simple view of data classification process

To formalize the proposed six-queue system, the state transition probability (P_{ij}), process birth (λ_i), and process death (μ_j) relation should be determined (see Eq. (1)).

$$P_{ij=}\lambda_i + \mu_j \tag{1}$$

In the proposed prioritization process, there are six queues (Q1, Q2, Q3, Q4, Q5, and Q6). Each queue is reserved for a special type of IoMT data (i.e., data class). Data can be transformed from one queue to another depending on its importance in a specific war time. This data

transformation process is achieved during the execution time. Listed below are seven steps that clarify how the prioritization process works:

a. The IoMT system data, which is incoming from the communication layer, is distributed over the six queues. This data will be classified within a specific interval by a war administrator system. P_1 to P_6 represent the classifier selection initial probabilities where $\sum_{i=1}^{6} Pr_i = 1$.
b. In the case of insufficient bandwidth or QoS deficiency for a current serviced data block, the system will select another block of data provided that the new data block can be found in the same queue as the old one.
c. In the case of incomplete data block processing, the data block will be transformed to a lower priority queue.
d. If Q6 is empty, the data blocks in Q1 (which has sufficient QoS) will be processed.
e. If Q1 is empty, the control will be transformed to Q2.
f. If any data block has an incomplete status, the data block will be transmitted to the next queue.
g. If the service control is at a queue and a data block comes to a higher priority queue, the control will jump to the higher priority queue immediately to service the new data block.

State Transitions

The Markov chain model should be defined in the proposed six-queue scheme. Each queue represents a state: state1 for Q1, state2 for Q2, state3 for Q3, state4 for Q4, state5 for Q5, and state6 for Q6. The required service time for one data block is determined by τ $(\tau = 1, 2, 3, \ldots)$. Each system state transition is considered to be either for waiting or for servicing. Fig. 5 shows the states' transitions.

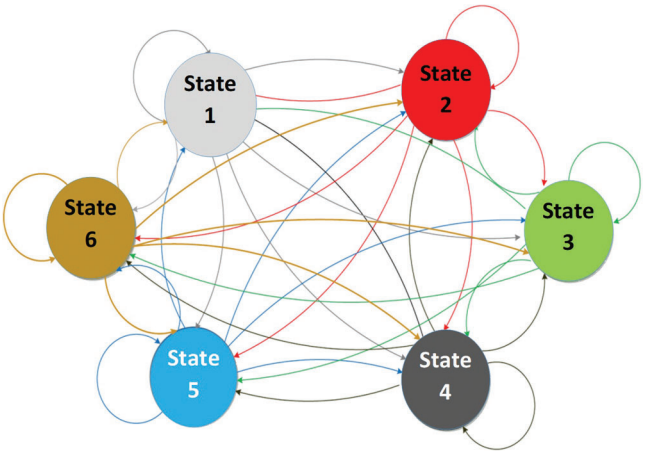

Figure 5: The queuing system states transitions

Suppose that $\{Y^{\tau}, \tau \geq 1\}$ is used to define the Markov chain where Y^{τ} is the queue that will be selected at a time τ^{th}. Let $\{Q_1, Q_2, Q_3, Q_4, Q_5, Q_6\}$ is space of the state for a random variable Y. The initial selection probabilities $(\sum_{i=1}^{6} Pr_i = 1)$ are determined using Eqs. (2) to (7).

$$P_{r1=}P\left[Y^0 = Q_1\right] \tag{2}$$

$$P_{r2=}P[Y^0 = Q_2] \tag{3}$$

$$P_{r3=}P[Y^0 = Q_3] \tag{4}$$

$$P_{r4=}P[Y^0 = Q_4] \tag{5}$$

$$P_{r5=}P[Y^0 = Q_5] \tag{6}$$

$$P_{r6=}P[Y^0 = Q_6] \tag{7}$$

S_{ij} ($i = 1, 2, 3, 4, 5$, and 6) represents the probabilities of system transactions over the six states. Tab. 1 represents the state transition matrix. The row-dependent model in Eq. 8 should be applied as well. Tab. 2 shows the proposed six-queue scheme.

$$P_{ij=}\lambda_i + i(\mu_j) \tag{8}$$

Table 1: The matrix of state transition

		Y^τ					
		Q_1	Q_2	Q_3	Q_4	Q_5	Q_6
$Y^{\tau-1}$	Q_1	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}
	Q_2	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}
	Q_3	S_{31}	S_{32}	S_{33}	S_{34}	S_{35}	S_{36}
	Q_4	S_{41}	S_{42}	S_{43}	S_{44}	S_{45}	S_{46}
	Q_5	S_{51}	S_{52}	S_{53}	S_{54}	S_{55}	S_{56}
	Q_6	S_{61}	S_{62}	S_{63}	S_{64}	S_{65}	S_{66}

Table 2: The proposed six-queue scheme analysis

		Y^τ					
		Q_1	Q_2	Q_3	Q_4	Q_5	Q_6
$Y^{\tau-1}$	Q_1	λ	$\lambda+\mu_j$	$\lambda+2\mu_j$	$\lambda+3\mu_j$	$\lambda+4\mu_j$	$1-(5\lambda+6\mu_j)$
	Q_2	$\lambda+\mu_j$	$\lambda+2\mu_j$	$\lambda+3\mu_j$	$\lambda+4\mu_j$	$\lambda+5\mu_j$	$1-(5\lambda+10\mu_j)$
	Q_3	$\lambda+2\mu_j$	$\lambda+3\mu_j$	$\lambda+4\mu_j$	$\lambda+5\mu_j$	$\lambda+6\mu_j$	$1-(5\lambda+14\mu_j)$
	Q_4	$\lambda+3\mu_j$	$\lambda+4\mu_j$	$\lambda+5\mu_j$	$\lambda+6\mu_j$	$\lambda+7\mu_j$	$1-(5\lambda+18\mu_j)$
	Q_5	$\lambda+4\mu_j$	$\lambda+5\mu_j$	$\lambda+6\mu_j$	$\lambda+7\mu_j$	$\lambda+8\mu_j$	$1-(5\lambda+22\mu_j)$
	Q_6	$\lambda+5\mu_j$	$\lambda+6\mu_j$	$\lambda+7\mu_j$	$\lambda+8\mu_j$	$\lambda+9\mu_j$	$1-(5\lambda+26\mu_j)$

3.3 The Application Layer

The application layer in the IoMT system architecture comprises heterogeneous applications used in war missions such as management, surveillance, etc. This layer should manage the functions of these applications using one general application without affecting their efficiency. The unification process of these applications should be achieved based on the communication data (message exchange). In data communication, output data for one application may act as input data for another application. Therefore, determination of input data and output data for war applications is considered one of the most important targets of this layer. For example, the input

of the rocket launch application of an aircraft or a launcher needs the output data of the satellite surveillance application, and the satellite surveillance application may need data from the WSN application. Communication between the information layer and the application layer is very important because the data, which will be considered as inputs and outputs, should be handled first in the information layer. Hence, to design the general application that will be used to manage the military applications, it should first determine input and output data for each application individually. Then, the time of data processing should be defined (hard, real, or soft). For example, in the case of a sudden change in the coordinates of a particular target during a cessation of fighting, three applications should interact in real time to achieve the mission and hit the target in its new position. These interacting applications make up the WSN, war management as well as cabin of the plane entrusted with the mission. The priority with which to apply special applications should be determined as well. For example, defense applications will have activation priority in cases of multiple enemy attacks on a particular target.

In accordance with the discussion above, the general management application should have a special database. This database stores dynamically changing data about individual military applications. This data is related to the following topics: Inputs and outputs, the data flow directions between individual applications, hard-time military situations, real-time military situations, soft-time military situations, and the priority for each application. These priorities should be determined based on war situations. The design of the IoMT system database may be distributed or central depending on the nature of the general management IoMT application. In a distributed database, the complexity of interaction between database servers should be noted, especially in case of events that require a hard-time or real-time interaction (see Fig. 6).

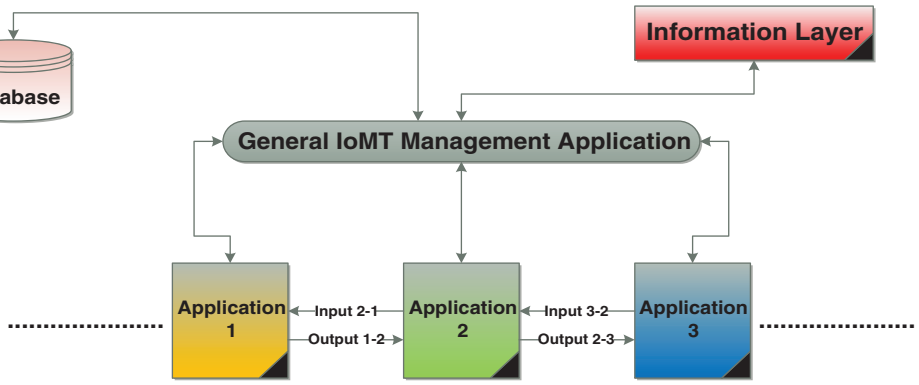

Figure 6: Simple view of the IoMT application layer

3.4 The Decision Support Layer

One of the most important issues in war is the decision-making process. In a technological war, a decision should have many specs such as accuracy, real-time, clearness, security, and fast distribution. All of these specifications should be related to the data that is gathered for the information layer. Although there is a close relationship between information and military decisions, the proposed IoMT system architecture has a middle layer between the information layer and the decision support layer called the application layer. The massive number of terabytes gathered within short periods should be analyzed, filtered, prioritized, and compressed. These processes are already achieved in the information layer. However, the information layer does not have the ability

to determine the direction of information moving between applications (i.e., the normal sequence of information). This sequence of information means that each data segment should be directed to a suitable application in order to become complementary and balanced. This information will be used in the decision-making process. For example, suppose that war managers have a goal that requires information to be processed in a specific arrangement and a particular order until a certain result is obtained from a military reconnaissance trip. The completion of that goal will be achieved through infantry and air defense. Therefore, the link between the application layer and the decision support layer will have a good impact on decision-making with high-precision specifications, which will be useful in critical war events.

Put simply, the decision support process outlined in this paper comprises five steps: Event weight, solution identification, choice of one solution, action, and output evaluation (see Fig. 7). The event weight can be extracted by war managers depending on their levels of experience. Once the event is well-understood, it is time to define solutions. There are many different alternatives available when a decision is prepared. Therefore, it is important to determine the range of available actions. Next, alternatives should be chosen and the risks of each alternative solution should be determined. Then, it will be time to take action. The implementation plan should be determined and the resources required to implement the selected solution should be available. Execution timing should be preciously determined, and then execution may begin. Finally, output of the selected solution implementation should be evaluated. Note that there are many decision support systems which may be implemented in the IoMT after they have undergone practical tests such as in [24,25].

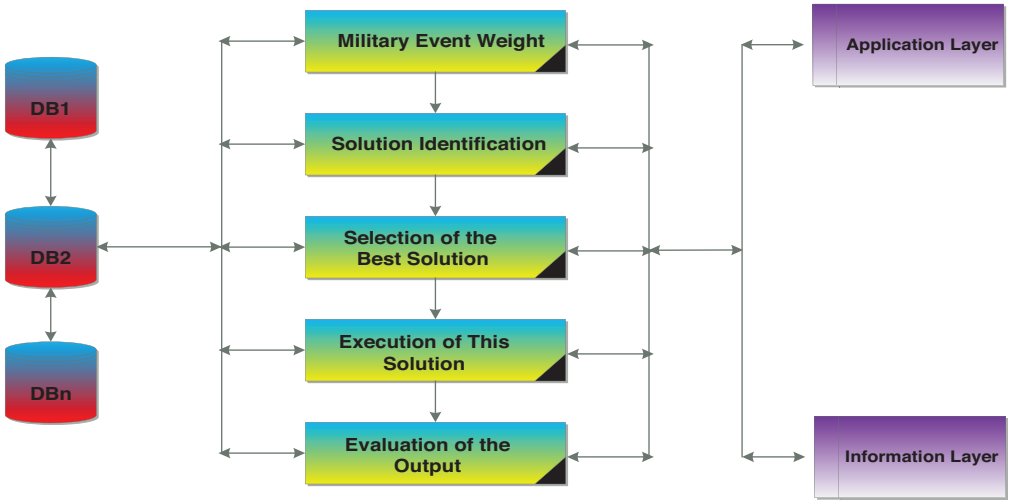

Figure 7: Simple view of the decision support layer

There are three main challenges which may be raised in the decision support layer. The first challenge is that of having too much or not enough data. This means that the decision support layer output will be late or inaccurate, which may cause a disaster because real-time decisions are needed in most times of war. The second challenge is problem misidentification. In most war missions, there are many issues surrounding a decision. However, sometimes there is nothing to confirm the truth of these issues. The third challenge is outcome overconfidence. Even if decision-making processes are implemented accurately, the actual output may not match up exactly

with the expected output. The application layer will face these challenges by determining the accurate information needed for decision construction, an accurate definition for the problem, and output adaptation. As a result, the output of the application layer will be used by the decision support layer. This makes the separation between these layers an important issue to consider in the proposed IoMT architecture.

4 Simulation and Evaluation

There are two main topics in this section: Construction of the simulation environment, and discussion of the simulation results. The simulation environment comprises five different main networks which are communicated with each other to construct the IoMT system.

4.1 Construction of the Simulation Environment

First, a military simulation environment should be constructed to test the performance of the proposed IoMT architecture. Network Simulator 3 (NS3), one of the most widely used network simulation packages, will be used to achieve this target. The military simulation environment comprised five different types of networks which include a huge number of nodes distributed over a large area. These five networks are WSN, RFID, MANET, HAP, and satellite networks. These networks are determined depending on battlefield requirements. The simulation, which stated in [26], is used to evaluate the proposed IoMT architecture. In WSN simulation, thousands of sensors in the war environment are distributed and deployed. One or more base stations are presented to connect these sensors with each other and gather information from them. In sudden events, the sensors able to send a trap message to the base station. Then, if the situation is urgent and requires that a decision be made quickly, the base station will send information directly to executers such as fighters, managers, etc. However, in a normal situation, the base station will resend gathered information (detailed or abstracted) to the manger(s) in charge for decision creation. The base station is supposed to be smart and programmed to achieve this target. For accurate WSN representation in the IoMT, the sensors should have various transmission ranges. For RFID, the best scenario was used by the United States military in the Second Gulf War [27]. One RFID tag should be attached to each soldier to be tracked into the battlefield. In addition, war tools such as commercial shipments and air pallets should be digitally tagged with RFID to know the up-to-date status of critical tools such as tanks and plans. Moreover, to save soldiers' lives, the proposed simulation system considers mobile hospitals that specialize in warfare and should be equipped with RFID technology. Furthermore, small inventory army things are observed using RFID technology to achieve tighter inventory control. For MANET simulation, it contains a temporary communication between battlefield objects such as vehicles, soldiers, and information providers. In some military cases, it is difficult to pass or send information through/to the data collection center. So, one from considerations in MANET simulation is to use this network in data transmission. The architecture stated in [28] is used to communicate HAP and satellite networks. The Internet simulation uses the routing algorithm presented in [29] and the IoT mixed multicast architecture stated in [30]. Multimedia transmission is achieved using [31], but the traditional military system is simulated using guidelines stated in [32,33].

IoMT data will be created randomly and dynamically for the information layer simulation. Then, this data will be classified and entered into queues where each queue will serve as a data class. Dynamic data creation depends on the war missions that are stored in a special database. The compression technique and the data filtering technique stated in [34] are used in this simulation scenario for data reduction, which represents one of the main targets in the information

layer. The application layer simulation also depends on the war missions, which comprise many scenarios for simulated networks. Input and output data are predetermined in a simulation file for each network application. Communication between the network applications and the general management application is achieved by message transmission. The simulation in [35] is used to cover the decision support layer. Part of war missions modeling and simulation are taken from [36], and the general specs of the weapons used in this simulation are taken from [37]. Fig. 8 shows a general view of the proposed IoMT system simulation environment.

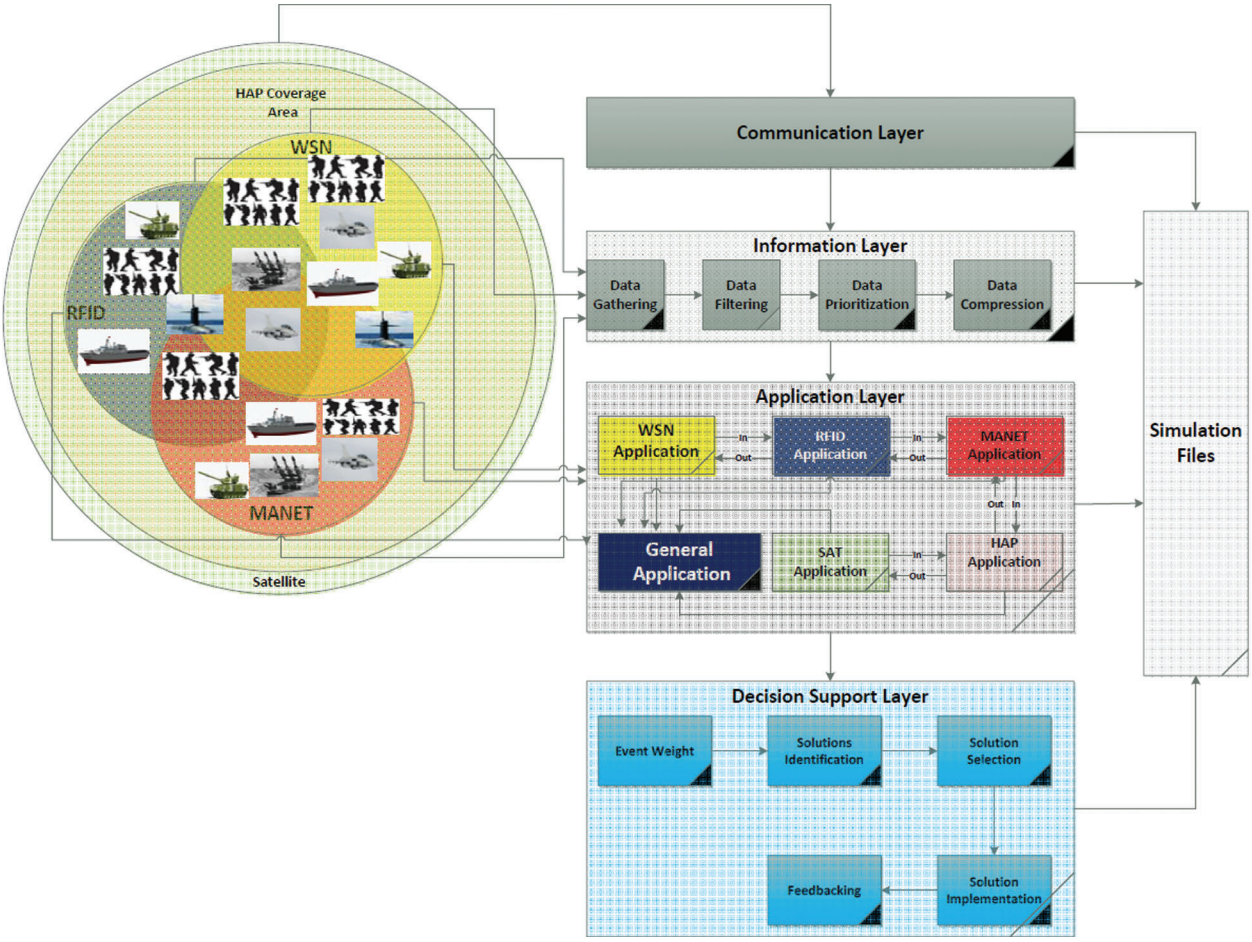

Figure 8: Simple view of the IoMT simulation environment

4.2 Results and Discussion

The performance metrics include packet loss, end-to-end delay, throughput, energy consumption, data reduction rate, and queue-type transformation. These performance metrics are selected to determine the effectiveness of IoT technology in the military environment. These performance metrics are measured for the IoMT system and compared with the traditional system. The traditional system uses traditional communication systems, algorithms, and techniques in war missions.

Packet loss is considered an important performance metric due to the sensitivity of each byte in the decision-making process of military missions. Due to the number of objects in the IoMT system, a massive number of megabytes can be transmitted within a short period. This may lead to high packet loss rates in the traditional military system, especially in network bottlenecks. This metric is measured by the number of packets received correctly at each destination. To determine the rate of packet loss over all of the IoMT system, the total number of lost packets is divided by the total number of sent packets. Fig. 9 shows the packet loss ratio after testing the IoMT system and the traditional system using the constructed simulation environment. In this figure, the x-axis represents the simulation time in minutes, and the y-axis represents the average packet loss values. A packet loss value is acquired each second, but the average packet loss value is calculated every minute. As shown in Fig. 9, the average packet loss value of the IoMT system is less than that of the traditional system. The hesitations in the IoMT system plot are smoother than those in the traditional system plot. This means that a sudden increase in the amount of data transmitted in a war mission produces high packet loss ratios at many simulation time points, such as time points 27 and 69, which can have a negative effect on decision-makers. On the other hand, the IoMT system can face this type of problem by decreasing the packet loss ratio, thus producing a positive effect.

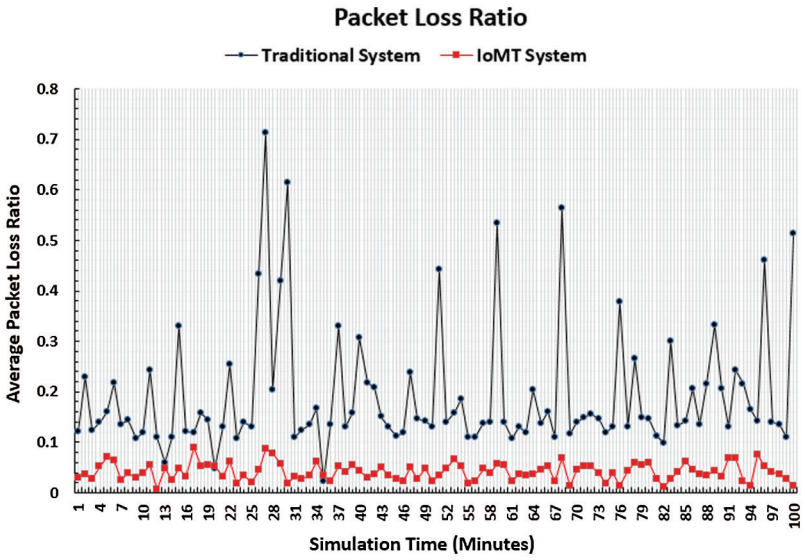

Figure 9: Packet loss ratio

The end-to-end delay performance metric reflects the efficiency of the IoMT system by decreasing the amount of time taken for data transmission, thus decreasing of the overall amount of time taken for data processing. Therefore, it is essential to measure this performance metric. The number of packets sent by sources and received by destinations in a predetermined amount of time is used to measure the end-to-end performance metric. The types of delays that are considered in calculating this performance metric include queuing, propagation, processing, and transmission. The results of this performance metric are shown in Fig. 10. In this figure, the x-axis represents the simulation time in minutes, and the y-axis represents the average end-to-end delay values. It is noticeable that the end-to-end delay values of the IoMT system are less than those of the traditional system. This can be explained by the amount of transmitted data that

has been reduced by IoMT methods and techniques, creating a greater range of transmitted data that is not found and saving a bandwidth for important packets to be served with accepted delay. Conversely, the traditional system may produce a massive number of megabytes, thus leading to overloaded transmission channels and congestion that would certainly lead to high end-to-end delay, especially in bottlenecks. Additionally, the end-to-end delay figure plots have many hesitations. This appears to be due to random events which may be constructed in the simulation environment to reflect the real nature of the IoMT system environment. These events may consume a network resource suddenly, leading to a sudden decrease in the QoS and a sudden increase in the end-to-end delay values that appear as hesitations in the Fig. 10 plots.

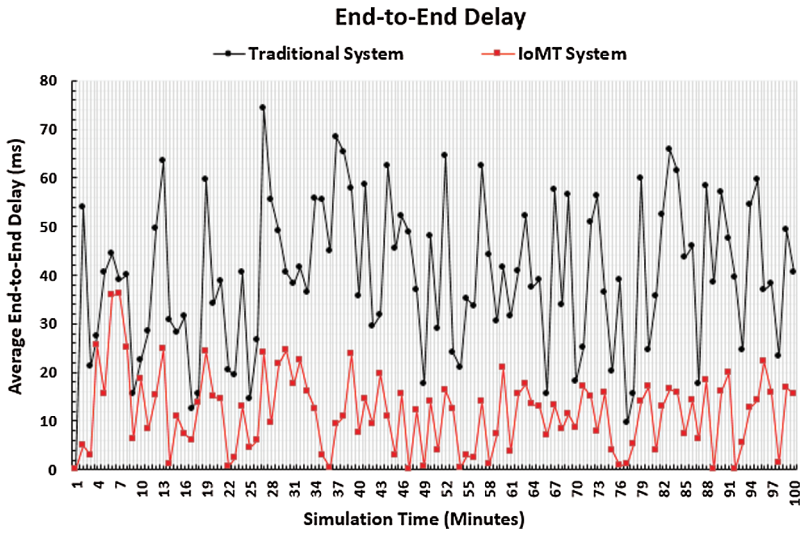

Figure 10: End-to-end delay

The throughput performance metric is used to determine the efficiency of the IoMT system, and is calculated using the total number of packets that are transmitted and received correctly by their destinations. The throughput performance results are shown in Fig. 11. The x-axis represents the simulation time in minutes, and the y-axis represents the throughput values in kB/s. It is notable that the throughput values produced by the IoMT system test are higher than those produced by the traditional system test. This means that the number of packets transmitted and received correctly is high in the IoMT system, which can be taken to mean that the IoMT system provides the transmitted packets with their required QoS. Conversely, the traditional system deals with the military mission as one status that is considered against the nature of the war. The transmitted packets may face many bottlenecks, which may lead to congestion and an increase in the number of lost packets, thus affecting the throughput. Additionally, the bottlenecks may increase delay, which would also affect the throughput.

Extension of network lifetime is an important target, especially in military missions. It is well-known that the network lifetime is related to the energy consumption of each energy-based network node. High energy consumption is associated with a low network lifetime, and vice versa. The core networks of the IoMT system include WSN, RFID, and MANET networks. Most of these networks' nodes are energy-based. Additionally, the number of bytes transmitted in the IoMT system is related to the energy consumption ratio. Therefore, measurement of the energy

consumption ratio of each network is a very important performance metric. Figs. 12–14 show the results of energy consumption in the WSN, RFID, and MANET networks respectively. The x-axis represents the simulation time in minutes, and the y-axis represents the average energy consumption. It is notable that the energy consumption rates of the three networks in the IoMT system test are less than those of the traditional network. This can be explained by the high number of transmitted packets in the traditional system that consume a large amount of energy. However, the number of transmitted packets in the IoMT system is controlled by the general health of the IoMT networks. This means that in cases of large energy consumption rates, the number of transmitted packets is dynamically decreased using the IoMT techniques described above.

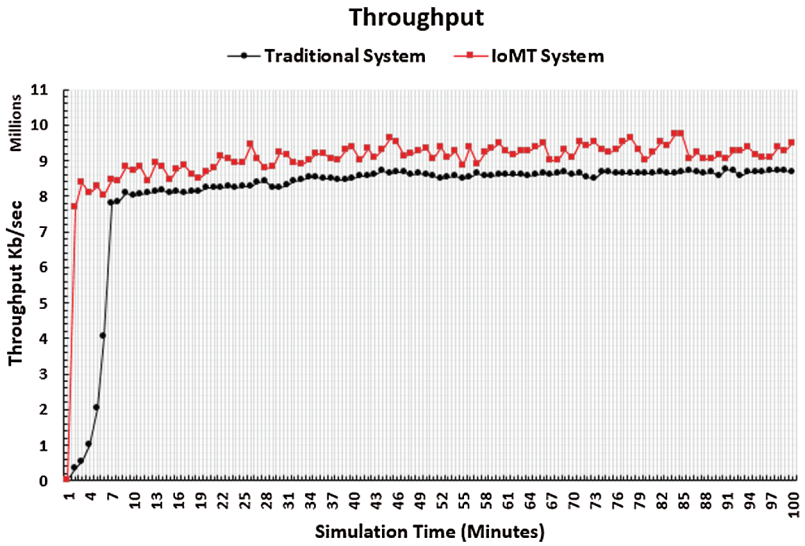

Figure 11: Throughput

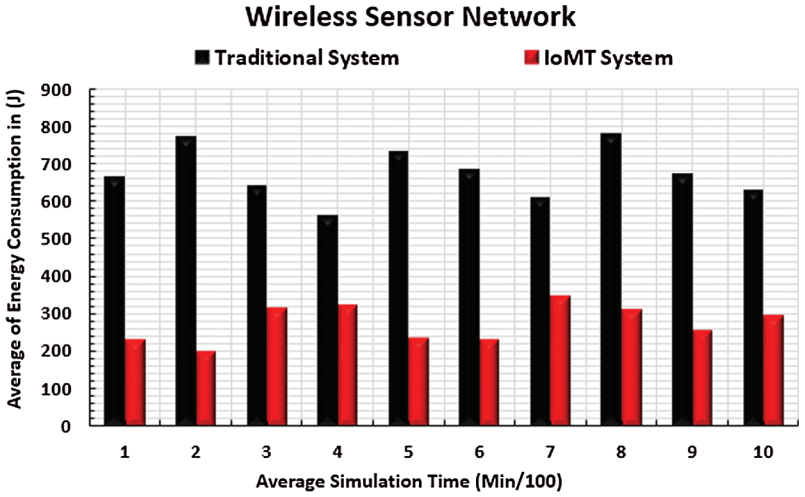

Figure 12: WSN energy consumption

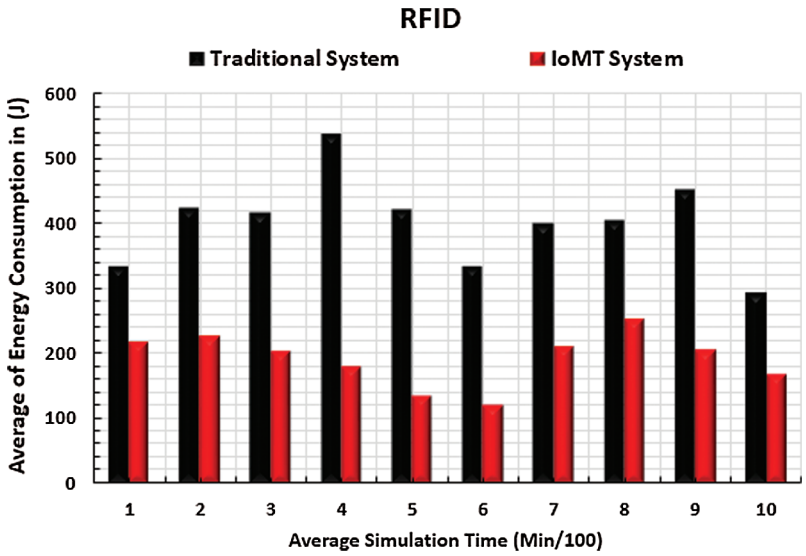

Figure 13: RFID energy consumption

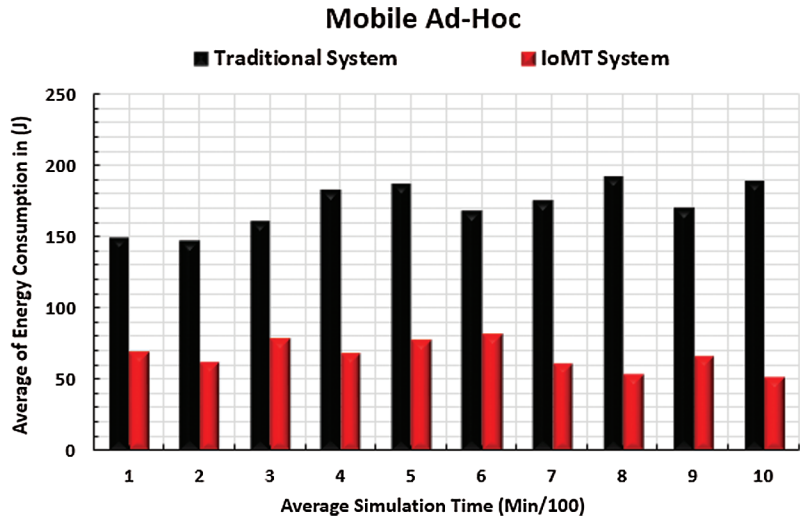

Figure 14: Mobile ad hoc energy consumption

The data reduction performance metric is important as well. This performance metric is measured by the total number of transmitted packets within the simulation time of IoMT and traditional systems. Fig. 15 shows the data reduction rate results of the simulation. The x-axis represents the simulation time in minutes, and the y-axis represents the reduction percentage of the IoMT system. There are notably different reduction rate percentages due to the existence of different IoMT statues. Furthermore, IoMT system data reduction is related to two parameters: The network QoS, and the number of packets transmitted over a period of time. Therefore, the quantity of data that should be reduced can be determined depending on the available QoS. The hesitations in the plots come from sudden changes in network size (join/leave objects), which affect the total number of transmitted packets.

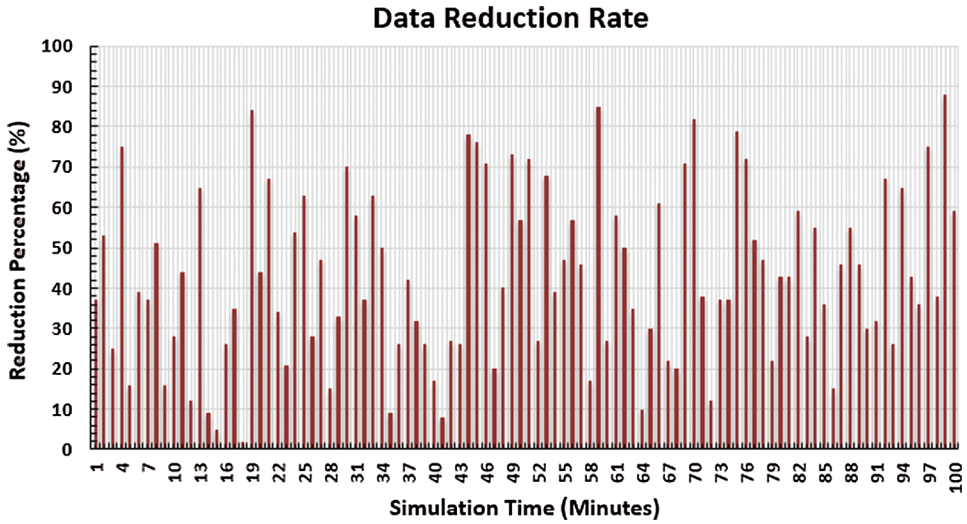

Figure 15: Data reduction rate

Finally, the transformation rate between queue types should be tested to make sure that the proposed data prioritization system is working in an efficient manner. This performance metric is measured by the period in which the IoMT system uses a special type of data prioritization queue. Fig. 16 shows the queue type transformation rate results of the simulation. The x-axis represents the queue type, and the y-axis represents the time percentage of queue type usability. The time period for the six-queue type is notably large. This can be explained by the nature of IoMT environment, which comprises massive amounts of data which must be prioritized into many types. The two-queue and three-queue types come in second order after the six-queue type. This means that the normal state of the IoMT environment requires less data prioritization. Diversity of queue type usage means that the data prioritization system depends on the size of data transmitted within the simulation periods.

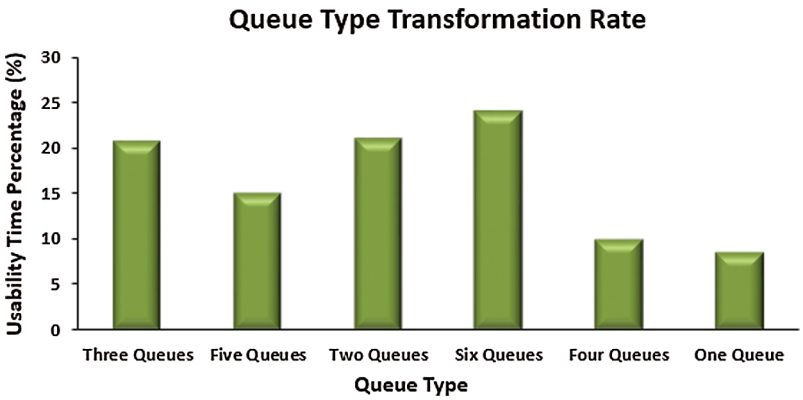

Figure 16: Queue type transformation rate

5 Conclusion

This paper proposes an IoT-based military system called the IoMT. The IoMT system architecture consists of four layers: Communication, information, application, and decision support.

The functions of each layer are demonstrated. A reliable coverage system is used for military objects. Additionally, a six-queue system is proposed to prioritize IoMT data. Data reduction techniques such as data filtering, data compression and data abstraction are used in the IoMT system. Moreover, the proposed IoMT system is sensitive to the QoS of its infrastructure networks. To test the performance of the proposed IoMT system, a simulation environment is constructed using NS3. The performance metrics used in this simulation environment include packet loss, end-to-end delay, throughput, energy consumption, data reduction percentage, and queue type transformation rate. The simulation results of the IoMT system are compared with those of the traditional system. Simulation results for each of the performance metrics proved that the IoMT system outperformed the traditional military system as follows: The packet loss percentage was decreased by 85.02%↓, the end-to-end delay percentage was decreased by 70.52%↓, the throughput percentage was increased by 89.62%↑, the percentage of energy consumption was deceased by 57.67%↓, and the average percentage of data reduction reached 42.77%↓. Moreover, the simulation results confirmed that the prioritization queue type may change with time. This gives the proposed IoMT system full flexibility in dealing with the sudden events that may occur in war missions. Therefore, the IoMT system is recommended to achieve the war management.

Acknowledgement: The authors extend their appreciation to Taif University Researchers Supporting Project Number (TURSP-2020/60), Taif University, Taif, Saudi Arabia.

Funding Statement: This work is funded by Taif University Researchers Supporting Project number (TURSP-2020/60), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Wang, Y. Tang, S. He, C. Zhao, P. K. Sharma *et al.,* "LogEvent2vec: LogEvent-to-vector based anomaly detection for large-scale logs in internet of things," *Sensors*, vol. 20, no. 9: 2451, pp. 1–19, 2020.

[2] M. Mohammadi, A. Al-Fuqaha, S. Sorour and M. Guizani, "Deep learning for IoT big data and streaming analytics: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2923–2960, 2018.

[3] A. Rahim, K. Ma, W. Zhao, A. Tolba, Z. Al-Makhadmeh *et al.,* "Cooperative data forwarding based on crowdsourcing in vehicular social networks," *Pervasive and Mobile Computing*, vol. 51, no. 11, pp. 43–55, 2018.

[4] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal *et al.,* "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[5] Y. Ren, F. Zhu, P. K. Sharma, T. Wang, J. Wang *et al.,* "Data query mechanism based on hash computing power of blockchain in Internet of Things," *Sensors*, vol. 20, no. 1: 207, pp. 1–22, 2020.

[6] A. Chatfield and C. Reddick, "A framework for internet of things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government," *Government Information Quarterly*, vol. 36, no. 2, pp. 346–357, 2019.

[7] J. Wang, W. Chen, L. Wang, R. S. Sherratt, O. Alfarraj *et al.,* "Data secure storage mechanism of sensor networks based on blockchain," *Computers Materials & Continua*, vol. 65, no. 3, pp. 2365–2384, 2020.

[8] S. Balaji, K. Nathani and R. Santhakumar, "IoT technology, applications and challenges: A contemporary survey," *Wireless Personal Communications*, vol. 108, no. 1, pp. 363–388, 2019.

[9] A. Badshah, A. Ghani, M. Qureshi and S. Shamshirband, "Smart security framework for educational institutions using internet of things (IoT)," *Computers Materials & Continua*, vol. 61, no. 1, pp. 81–101, 2019.

[10] J. Sheu, I. Chen and Y. Liao, "Realization of internet of things smart appliances," *Intelligent Automation and Soft Computing*, vol. 25, no. 2, pp. 395–404, 2019.

[11] A. Lele, "Disruptive technologies for the militaries and security, part of the smart innovation," *Systems and Technologies Book Series*, vol. 132, pp. 187–195, 2018.

[12] K. S. Chan and F. T. Johnsen, "Military communications and networks," *IEEE Communications Magazine*, vol. 58, no. 8, pp. 13, 2020.

[13] B. Jalaian and S. Russell, "Uncertainty quantification in internet of battlefield things," in *Artificial Intelligence for the Internet of Everything*, Academic Press, pp. 19–45, 2019, ISBN: 9780128176368, https://doi.org/10.1016/B978-0-12-817636-8.00002-8, http://www.sciencedirect.com/science/article/pii/B9780128176368000028.

[14] L. Yushi, J. Fei and Y. Hui, "Study on application modes of military internet of things (MIOT)," in *IEEE Int. Conf. on Computer Science and Automation Engineering*, Zhangjiajie, China, pp. 630–634, 2012.

[15] J. Chudzikiewicz, J. Furtak and Z. Zielinski, "Fault-tolerant techniques for the internet of military things," in *IEEE 2nd World Forum on Internet of Things*, Milan, Italy, pp. 496–501, 2015.

[16] J. Głowacka, J. Krygier and M. Amanowicz, "A trust-based situation awareness system for military applications of the internet of things," in *IEEE 2nd World Forum on Internet of Things*, Milan, Italy, pp. 490–495, 2015.

[17] A. Kott, A. Swami and B. West, "The internet of battle things," *IEEE Computer*, vol. 49, no. 12, pp. 70–75, 2016.

[18] M. Tortonesi, A. Morelli, M. Govoni, J. Michaelis, N. Suri *et al.,* "Leveraging internet of things within the military network environment—Challenges and solutions," in *IEEE 3rd World Forum on Internet of Things*, Reston, VA, USA, pp. 111–116, 2016.

[19] M. Pradhan, F. Gökgöz, N. Bau and D. Ota, "Approach towards application of commercial off-the-shelf internet of things devices in the military domain," in *IEEE 3rd World Forum on Internet of Things*, Reston, VA, USA, pp. 245–250, 2016.

[20] M. Dyk, M. Chmielewski and A. Najgebauer, "Combat triage support using the internet of military," in *Federated Conf. on Computer Science and Information Systems*, Prague, Czech Republic, pp. 835–842, 2017.

[21] B. Jalaian, T. Gregory, N. Suri, S. Russell, L. Sadler *et al.,* "Evaluating LoRaWAN-based IoT devices for the tactical military environment," in *IEEE 4th World Forum on Internet of Things*, Singapore, pp. 124–128, 2018.

[22] F. Johnsen, Z. Zieliński, K. Wrona, N. Suri, C. Fuchs *et al.,* "Application of IoT in military operations in a smart city," in *Int. Conf. on Military Communications and Information Systems*, Warsaw, Poland, 2018.

[23] S. Srivastava, M. Singh and S. Gupta, "Wireless sensor network: A survey," in *Int. Conf. on Automation and Computational Engineering*, Uttar Pradesh, India, pp. 159–163, 2018.

[24] G. Cai, G. Li and Y. Dong, "Decision support systems and its application in military command," in *2nd Int. Conf. on Consumer Electronics, Communications and Networks*, Yichang, China, 2012.

[25] M. Frey and A. Schulte, "Tactical decision support for UAV deployment in MUM-T helicopter missions: Problem analysis and system requirements," in *IEEE Conf. on Cognitive and Computational Aspects of Situation Management*, Boston, MA, USA, 2018.

[26] O. Said and A. Tolba, "DORS: A data overhead reduction scheme for hybrid networks in smart cities," *International Journal of Communication Systems*, vol. 33, no. 12, pp. e4435, 2020.

[27] E. Peltz, J. M. Halliday, M. L. Robbins and K. J. Girardini, "Sustainment of army forces in operation Iraqi freedom battlefield logistics and effects on operations. Published by the RAND Corporation, 2005. [Online]. Available: https://www.rand.org/content/dam/rand/pubs/monographs/2006/RAND_MG344.pdf.

[28] O. Said and A. Tolba, "Performance evaluation of a dual coverage system for internet of things environments," *Mobile Information Systems*, vol. 2016, Article ID 3464392, 2016. https://doi.org/10.1155/2016/3464392.

[29] O. Said, "Analysis, design and simulation of Internet of Things routing algorithm based on ant colony optimization," *International Journal of Communication Systems*, vol. 30, no. 8, pp. e3174, 2017.

[30] O. Said and A. Tolba, "Design and performance evaluation of mixed multicast architecture for internet of things environment," *Journal of Supercomputing*, vol. 74, no. 7, pp. 3295–3328, 2018.

[31] O. Said, Y. Albagory, M. Nofal and F. Al Raddady, "IoT-RTP and IoT-RTCP: Adaptive protocols for multimedia transmission over internet of things environments," *IEEE Access*, vol. 5, pp. 16757–16773, 2017.

[32] J. Padilla, "Military simulation systems," *Engineering Principles of Combat Modeling and Distributed Simulation*, Wiley, pp. 851–868, 2012, ISBN: 9781118180310, https://doi.org/10.1002/9781118180310.oth2.

[33] K. Kang and R. Roland, "Military simulation, Chapter 19," in *Handbook of Simulation: Principles, Methodology, Advances, Applications, and Practice*. Hoboken, New Jersey, United States: John Wiley & Sons, 1998.

[34] O. Said, A. Elnashar and O. Elshakankiry, "Optimized mechanism for minimizing data overhead in IoT environments: Design, simulation and performance evaluation," *International Journal of Applied Engineering Research*, vol. 12, no. 23, pp. 13663–13676, 2017.

[35] Z. Han, "Modeling method and application of multi-agents in armored force operation simulation," in *IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conf.*, Chongqing, China, 2017.

[36] X. Li, J. Liu, S. Dang and X. Xie, "Designing of virtual battlefield operations by ABMS method," in *2nd Int. Conf. on Multimedia and Information Technology*, Kaifeng, China, 2010.

[37] Military Equipment Guide. [Online]. Available: https://www.military.com/equipment (Accessed 28 January 2021).