

CONTEXT INFORMATION AGGREGATION MECHANISM BASED ON BLOOM FILTERS (CIA-BF) FOR HIGH PERFORMANCE MONITORING APPLICATIONS OF INTERNET OF THINGS

Fawaz Alassery and Maha M. Althobaiti

College of Computers and Information Technology, Taif University, Taif, Saudi Arabia

ABSTRACT

Internet of Things (IoT) has become a popular technology in recent years. Different IoT applications such as traffic control, environment monitoring, etc. contain many sensor devices, routers, actuators, edge routers, and Base Stations (BS) which communicate with each other and send millions of data packets that need to be delivered to their destination nodes successfully to ensure the High-performance communication networks. IoT devices connect to the Internet using wired or wireless communication channels where most of the devices are wearable, which means people slowly move from one point to another or fast-moving using vehicles. How to ensure high performance of IoT data networks is an important research challenge while considering the limitation of some IoT devices that may have limited power resources or limited coverage areas. Many Kinds of research focus on how to customize routing protocols to be efficient for IoT devices. The traditional routing mechanisms utilized specific IP addresses to identify users while in IoT it is more beneficial to identify a group of users (things) based on any contexts, status, or values of their resources such as the level of their batteries (e.g., low, medium or high). While IoT devices have different characteristics, a multicasting mechanism to send one message to various groups of devices will not be efficient in IoT communication networks since the aggregation of packets is very difficult. Thus, it is useful to propose a mechanism that able to filter data packets that need to be sent to a specific group of devices. In this paper, we propose efficient context-aware addressing mechanism, which is based on bloom filters to increase the performance of IoT communication networks. A routing architecture is built based on bloom filters which store routing information. In our works, we reduce the size of routing information using a proposed aggregation mechanism which is based on connecting each group of IoT devices with an edge router which is hierarchically connected to an upper router after operating its bloom filter. Our simulation results show a significant improvement in the IoT performance metrics such as packets transmission delay, jitter the throughput, packets dropping ratio, and the energy consumption in comparison with well-known routing protocols of IoT such as Destination Sequenced Distance Vector routing protocol (DSDV), and Ad hoc On-demand Distance Vector routing protocol (AODV).

KEYWORDS

Internet of Things, context-aware addressing, bloom filters, High-performance IoT, routing in IoT. Packets aggregation mechanism.

1. INTRODUCTION

In recent years, the Internet of Things (IoT) has gained much attention in the scientific research community as a digital ecosystem. It is a field that concentrates on allowing objects to interconnect, exchange data, and share information over private or public Internet Protocol (IP) networks. These interconnected objects might be physical or virtual according to the object's tangibility, such as robots, people, sensors, buildings, enterprises, and the cloud [1]. The IoT has

been adopted widely into a variety of smart systems, such as healthcare, cities, agriculture, energy, and transportation [2][3], as shown in Figure 1. According to a Cisco white paper, remarkably, there will be an estimated 29.3 billion connected devices by 2023 [4], while in 2003, there were 500 million interconnected devices [5]—all of which reflect the power of IoT and how modern life depends on technologies. Inevitably, the IoT is considered one of the pervasive paradigms that contribute to increasing the information value generated by billions of interconnected devices. These devices involve people, businesses, services, and applications. In the latest survey by the McKinsey Global Institute, the economic value generated through the IoT may exceed \$11.3 trillion across different applications and technologies [6].

The IoT was named by Kevin Ashton in 1999 in a presentation title at Procter Gamble [7] to refer to the interconnection of objects via the Internet [8]. Reviewing more recent literature, the *Internet of Things* was defined by the International Telecommunication Union (ITU) as “a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving information and communication technologies” [9]. The three distinguishing features of the IoT are interconnectivity between billions of devices, heterogeneity, and dynamic change, which relate to the state of the device [9,10]. The basic concept in IoT is based on communication (transmitting data between two things) resembling a machine-to-machine (M2M) connection. However, the core idea of the IoT is to provide not only M2M connections but also human-to-machine (H2M) and human-to-human (H2H) connections while creating ease of communication that supports the provision of more convenient network services for users.

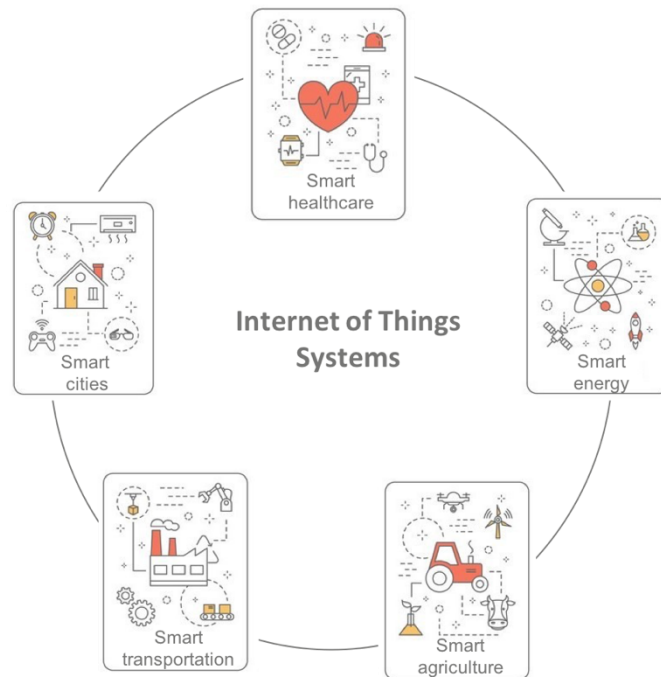


Figure 1. IoT Applications.

Also, the *routing mechanism* refers to establishing and selecting the best path (route) between devices (nodes) [11]. In the IoT, routing concentrates on transferring data (optimal packets) continuously through the network from one node to another with the least possible required resources [12]. Extensive research has been devoted to routing protocols to facilitate the transmission of packets between nodes. Efficient protocols have been produced to generate an

intelligent routing topology that minimizes the energy that will further support the reduction of the power consumption of IoT devices used to build a smart environment. Internet Engineering Task Force (IETF) groups have designed various IoT protocols in network layer communication [13]:

- IPv6 over Low-Power Personal Area Networks (6LoWPAN),
- Routing Protocol for Low-Power and Lossy Networks (RPL), and
- IPv6 over the Time-Slotted Channel-Hopping Mode of IEEE 802.15.4e (6TiSCH).

IPv6 over the 6LoWPAN proposed by the IETF 6LoWPAN working group is considered the key to building the IoT network and is based on transmitting large-sized IPv6 packets in IEEE 802.15.4 [14]. The paradigm of 6LoWPAN is based on using limited processing capabilities in low-power devices, and it has many distinctive characteristics to become a network technology suitable for IoT applications, such as low-cost, low-power, battery-supplied, IP-driven devices. The routing RPL proposed by the ROLL (Routing Over Low Power and Lossy Networks) working group in IETF for an IPv6 routing protocol for Low-Power Lossy Networks (LLNs) has the remarkable capability to build specific routes and distribute information to other nodes efficiently [15]. RPL is designed to support complex traffic models such as point-to-multipoint and multipoint-to-point as well as the simple pattern point-to-point. The authors in [16] compared in detail the IoT network layer protocol, including 6LoWPAN and RPL, according to nine parameters, and they mentioned that both 6LoWPAN and RPL enabled IPv6 connectivity to guarantee global reliability, reachability, scalability, and network security. The last-mentioned protocol in the list above is IPv6 over the Time-Slotted Channel Hopping mode of IEEE 802.15.4e (6TiSCH). This is the latest standard that IETF developed that combines IETF's upper stack that provides IPv6 connectivity, including RPL and 6LoWPAN, with the industrial performance of IEEE802.15.4 TSCH to be used for IoT devices [17], as seen in Figure 2.

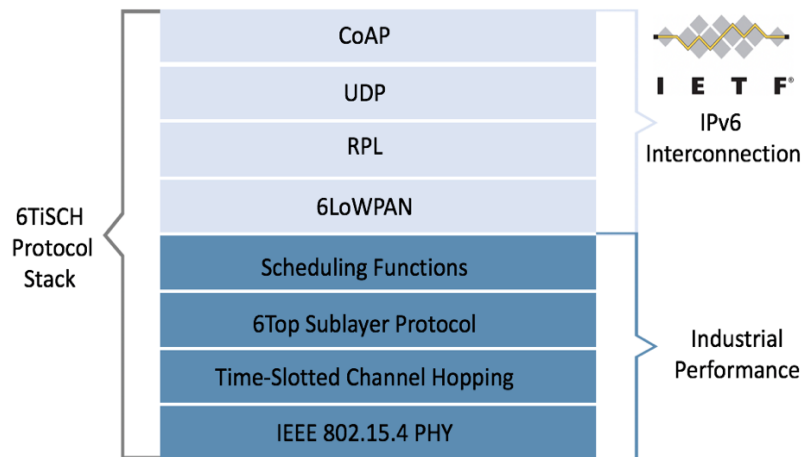


Figure 2. Routing protocols.

Routing plays a vital role in the IoT, and to fulfill the full functionalities of the IoT, efficient and scalable routing protocols are needed. The authors in [18] surveyed of most of the factors that affect the routing protocols used in IoT networks. These challenging factors include context awareness, node death, scalability, latency, heterogeneity, topology changes, incentive-based routing, data security, congestion control, data redundancies, and multipath routing. They also classified most of the factors that affect the routing process of the IoT, including devices, networks, resources, manufacturers, connectivity, the communication process, cooperation in data reliance, network topology, communication range, harsh environmental conditions, and

addressing mechanisms [18]. To address mechanisms considered among the context parameters of IoT devices, the authors emphasized that there should be an acceptable and universal unique addressing mechanism to ease M2M communication.

To deal with the above challenges, the main contributions of this paper are twofold:

- We proposed a context information aggregation mechanism using bloom filters where routers operate their bloom filter to send receiving packets to upstream routers after aggregating packets.
- We attached a 10-bits array in every transmitted packet which represents the current status of the IoT device. We mapped these 10-bits arrays into the bloom filter to specify the current context information for fast and efficient energy consumption.
- We compare our proposed CIS-BF mechanism with well-known routing protocols in IoT (i.e. DSDV and AODV) protocols. We show how our proposed mechanism outperforms DSDV and AODV protocols in terms of packets transmission delay, jitter, throughput, packets dropping ratio, and the energy.

The remainder of this paper is organized as follows. Section 2 reviews recent related works in context-aware addressing in IoT networks and dig deeply in the concept of bloom filters. Section 3 describes the benefits of using bloom filters in the routing of IoT. We also explained the main assumption that we present in our design based on the context information aggregation mechanism. Section 4 discusses the network communication model of our proposed context information aggregation mechanism based on the bloom filter (or CIA-BM mechanism). The evaluation results which show the advantages of the proposed CIA-BM mechanism are presented in section 5. We show five performance metrics (i.e. packets transmission delay, jitter, throughput, packets dropping ratio and the energy consumption). Finally, the conclusion of our paper is in section 6.

2. RELATED WORKS

In this section, we cover some related works in context-aware addressing as well as the main concepts in Bloom filters.

2.1. Context-Aware addressing

With the advent of the IoT, the relevance of routing schemes has increased significantly, which further attracted researchers to study this field. The basic scenario of IoT is based on the communication between two devices; therefore, many researchers focus on identifying information related to the communication between two devices, which refers to the context-aware concept to improve the routing decision process. There are various benefits of understanding context-aware routing, including intelligent routing, network lifetime maximization, network load balancing, and fewer communication delays [18].

The notion of context is the organized collection of information that can characterize an entity and its surrounding environment [19]. An entity can be an object, person, or place considered part of the interaction between the user and an application [20, 21]. In the case of the IoT, the entity is the node in the network, while the information distributed among the network nodes can be retrieved from an internal position (sensor nodes) or external position (from the environment or neighbor node) [22]. The contextual information in the IoT includes memory, the residual energy of the device, processing power [11] storage capabilities, link costs, nodes' velocity, the distance between nodes [23], speed of mobility, and battery [22]. Moreover, the message transmitted

between nodes has related contextual information, such as destination, priority, name of the source, and delivery deadline [23]. Regarding the environmental context, location information is considered the main context parameter [24, 25]. The authors in [26] used location information in designing a scheme that aims to query location-based services.

According to IEEE 802.21, we can collect contextual information from the network side and the client side [27]. Generally, using context criteria introduced “context-aware routing” because using these criteria enhances the routing process in different ways, such as minimizing communication delays and maximizing the network’s lifetime. However, some main challenges that influence context-aware routing. The authors in [11] identified three. The first is context acquisition, where the raw data of a context must be collected from the environment and converted to the context via the network topology. The second challenge is the quality of context (QoC), which is based on the quality of information extracted from the sensor, including accuracy, validity time, and resolution. Finally, context storage refers to the approaches used to store the context on devices.

Researchers have tended to focus on context because it influences routing performance. According to the context parameters collected from the network, the routing decision can take place. The authors in [28] conducted early work on context-aware routing. They introduced an intelligent mobile ad hoc network routing system that uses the most important parameters that affect the network context. The proposed system acquires the network’s performance and decides the routing protocol that provides better performance according to the network context, such as mobility and the number of nodes [28]. Another study by the authors in [29] presented a mechanism that uses two contextual information velocities and the distance between nodes to determine the lifetime of the network. They named their approach *context-aware routing for a P2P network on a mobile ad hoc network*, and it gave good results in reducing the probability of route failure [29].

Reviewing other recent studies, several context-aware mechanisms have been proposed, but without considering IoT networks. For example, the authors in [30] proposed a context-aware adaptive opportunistic scheme that provides good routing performance and efficient energy for wireless sensor networks (WSNs) using context parameters such as the progress of the message, energy, link quality, and validity of the scheme. In [31], a context-aware routing protocol for opportunistic CARTOON (Context-Aware Routing Protocol for Opportunistic Networks) has been proposed by a group of researchers after a series of experiments with various routing protocols to assess their effects on the performance level. The proposed protocol based on the experiment’s results used contextual information (i.e., the level of nodes’ density) to change between two modes (i.e., epidemic and probabilistic). They compared the performance of CARTOON with other well-known protocols, and it performed quite well. In another recent study on a Delay-Tolerant Network (DTN), the authors in [32] proposed an energy-aware protocol called EA-PRoPHET (Energy Aware Probabilistic Routing Protocol using History of Encounters and Transitivity) based on PRoPHET that used contextual information like the number of nodes, energy, and the free buffer of nodes to decide the storage of forwarded messages. The results showed an extension of the network’s life and improved the delivery of messages. Another protocol using context-aware was proposed by Rosas et al. in [33], called CSAR, or Context-aware Self-Adaptive Routing for DTNs. The proposed model is based on context and metric concepts. The contextual information of a node and its environment include the density of the environment, mobility, and energy availability. The metric is the performance quantification of a protocol of a context, including delivery rate, the latency of messages, and the average time of waiting messages. The model created a family of hybrid protocols that can be assessed for each node in the network after changing the metrics to select the best routing protocol.

Some context-aware works focus merely on IoT networks. For instance, the authors in [34] presented a Scalable Context-Aware Objective Function (SCAOF) that used context-aware features such as the node state, remained energy, and hardware/software reliability taken locally by the nodes to enhance the RPL-based model Routing Protocol for Agricultural Low-power and Lossy Networks (RPAL). The proposed solution provides efficient energy and quality of services (QoS) for Agricultural Low-power and Lossy Networks (A-LLNs). In [35], the authors introduced a context-aware trust management system for the IoT that uses some contextual information to evaluate the trust level of a node based on its past behavior. The main aim of the proposed system is to manage cooperation in heterogeneous IoT architecture. To design the system, the author's assigned trust scores to cooperate nodes according to the status of the neighbor node and other functions to improve the system's operation [35]. To deal with the problem in RPL routing protocols related to the dynamic and heavy load of IoT networks, Taghizadeh et al. [36] introduced a Context-aware and Load balancing (CLRPL) Routing Protocol. The proposed protocol aims to solve two main problems: reducing the rate of packet loss and increasing the network's lifetime through three stages. First, they proposed a new objective function called the Context-Aware Objective Function (CAOF) using contextual information such as the remaining power of the node and its parent based on the Expected Transmission Count and the parent's rank. In the second stage, they proposed a Context-Aware Routing Metric (CARF) that uses contextual information such as the state of the remaining energy and queue utilization of the parent chain in the path. Throughout the assessment, the chosen context metric gives an adequate decision about the best parent in a network with high traffic dynamicity. The third stage involves proposing a new algorithm to select the best parent based on CARF and other metrics and evaluating the proposed protocol in different scenarios. It showed good results in reducing energy consumption and increasing packet loss rate [36]. In [37], the authors overcome the problem of how to select the best sensor in IoT networks from millions of sensors by presenting a technique called Skyline query that can efficiently seek and select the best sensor based on contextual properties. Araujo et al. [38] proposed a mechanism for improving route selection based on contextual information in the domain of the IoT network. The proposal aims is to enhance the performance of the network; thus, the new mechanism involves designing four Delivery Quality and Context-Aware Objective Functions (DQCA-OFs) that use three metrics: number of hops, expected transmission count (ETX), and energy consumed. Moreover, to decide the best route, the authors have designed a route classifier based on a fuzzy system that can estimate the level of quality of the route in IoT scenarios. The results from the current study confirm that the proposed approach increases reliability, QoS, and network lifetime and minimizes the delay. In [39], the authors proposed an energy-efficient and Path Reliability Aware Objective Function (ERAOF). The proposed objective function aims to achieve high reliability and efficient energy for IoT applications using a combination of two main metrics, the ETX when deciding the selected route and the Energy Consumed (EC). The results confirmed a reduction in the number of packet losses due to the use of the ETX and EC, which in turn improved the network's performance.

In our design, we use Bloom filters in routing packets of monitoring applications for IoT.

In the following subsection, we will present a broader view of probabilistic data structures (PDS) and review the relevant prior research that draws on PDS.

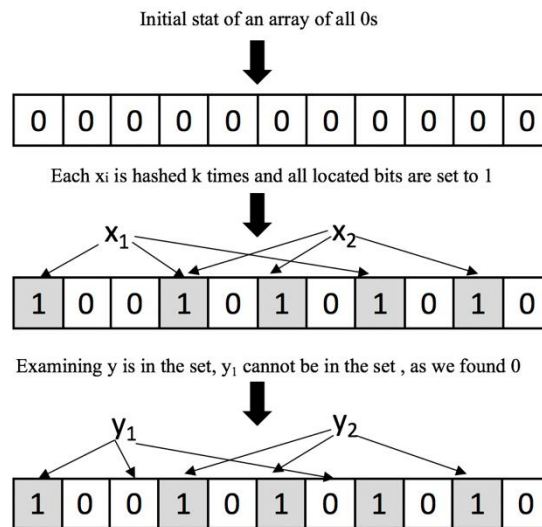
2.2. Bloom Filters Principle

Probabilistic data structures are a way to handle the vast amount of data using hash functions to randomize elements. There are various PDSs, such as a Bloom filter, quotient filter, and HyperLogLog (HLL) [40]. However, the Bloom filter (BF) is considered one of the most popular probabilistic membership data structures and has been extensively applied in many studies, as it

can perform a complex query in a very short time. It refers to an efficient approach to identify a set of items and recognize if a certain input belongs to a set [41, 42]. Burton Bloom introduced Bloom’s filter in the 1970s, and it is used quite widely in the database and networking literature. According to [43], a Bloom filter can be used in summarizing the content of peer-to-peer networks, locating source routing, simplifying packet routing protocols, and measuring infrastructure in network devices. Moreover, Bloom filters play a vital role in speeding up the packet process in software-defined networks [44].

In this section, we present the mathematical principle behind Bloom filters. The Bloom filter is applied to represent a set $S = \{x_1, x_2, x_3, \dots, x_n\}$ of n elements described by an m bit long array, where each bit in the initial step is set to 0. To execute the mapping procedure, the filter will use k independent hash functions h_1, \dots, h_k with the value range $\{0, 1, \dots, m\}$, and each hash function maps each element in the universe to a random number uniformly over the range. Specifically, for each element $x \in S$, the bits' $h_i(x)$ is set to 1 for $1 \leq i \leq k$. If we want to check if an item y is in S , we will use the hash functions $h_i(y)$ and examine the BF regarding whether the bits at positions are set to 1. If any of them is not set to 1, y is definitely not a member of S , but in case all instances of $h_i(y)$ ($1 \leq i \leq k$) are set to 1, we assume that y is in S with a non-zero probability that it is still not (see Figure 3). The assumption of this case is called a *false positive*, whereby an element y is in S even though it is not in Figure 3. A false positive (*fp*) can be expressed mathematically as follows:

$$fp = (1 - e^{-kn/m})^k$$



Within the domain of the IoT, several works have applied BFs; for instance, the authors in [45] discussed the privacy and security issues of fog computing in the IoT. They have proposed a schema that aims to improve the security of IoT devices through the distribution of certificate revocation information. The schema used Bloom filters to initiate a list that can effectively reduce the size of the revocation list. It has been used to search for a certificate identity; therefore, when two devices communicate in IoT networks, it needs to verify the certificate using a Bloom filter. If the identity is not included in the bloom, the certificate is considered revoked. Otherwise, the certificate is revoked, or the bloom gives a false positive state [45]. Moretti et al. [46] introduced the DIstributed Naming Service (DINAS) for the IoT based on three aspects using Bloom filters

to create compact names from node descriptions, designing a strategy for the propagation of name-address queries, and distributing stored names based on name similarity. In another related work [47], the authors proposed an approach for Software-Defined Networking to detect Man in the Middle attacks based on the OpenFlow control channel. The Bloom filter has been implemented in the system prototype by extending the OpenFlow mechanism to detect packet modification, and the results from the evaluation stage approve the efficiency of using a Bloom filter.

3. USING BLOOM FILTERS IN IOT ROUTING

In data networks, the aggregation of multicast addresses is so difficult in routing tables since each multicast group must have a different entry in the routing table which is different from the routers that are located all the routs from a source to a destination. In multicasting, different groups may have different members, and these groups are divided into various locations on the networks, so in the case of IoT, it is usual to send the data packets to separate groups of specific members while preventing the packets from being reached to other members. Also in IoT, the number of groups is increased rapidly as the need for sending millions of packets is the usual behavior of IoT technology [1].

Thus, using Bloom filters may bring an efficient mechanism in IoT since Bloom filters utilize the probabilistic data structure that can filter receiving packets and determine if a member must receive the transmitted packet which is directed to a specific group. In Bloom filters, considering false positive probability is possible where in multicasting scenario packets may reach to different groups even if some members are not intended to receive such packets. However, much more information can be stored in the routers that are distributed in the network areas [1].

In our design of using Bloom filters in routing packets of monitoring applications for IoT we assume the following:

- All the identifiers of non-aggregated IoT devices are advertised to intra-domain networks.
- Routers are distributed in the sensing area, which has Bloom filters to store the routing information of devices that are located in the routing path to these routers. Routers form a hierarchical topology to connect a router in levels for sending packets to up/down routers.
- Each router has its k hash function and the same filter size x . Moreover, routers that are located to each group of IoT devices will receive packets from that group. In other words, each edge network sends its packets to closer routers that have bloom filters.
- Each router operates its own Bloom filter in order to send receiving packets to upstream routers after aggregating packets (figure 4). When a packet arrives in a router with identifier I (i.e. represents a specific identifier for each device in a network e.g. IP address), the router checks in its bloom filter to find the matched identifier to direct the packet to the correct upstream router for next-hop forwarding.

4. THE NETWORK COMMUNICATION MODEL

In this section, we discuss how to rout packets inside and outside the distributed groups of IoT devices where packets are targeted to reach the destination node as will be explained in the performance evaluation section.

In our design, each group has IoT devices that are distributed in the geographical area for the purpose of monitoring physical phenomena. IoT devices send periodic (or priority) messages to a specific destination which are located far away from the sensing area. These IoT devices have

limited power resources, such as pre-defined battery levels. In our work, It is mandatory to propose a routing mechanism that aims to extend the battery lifetime of IoT devices and give priority for some urgent messages in monitoring applications, and hence increase the performance of the whole IoT networks.

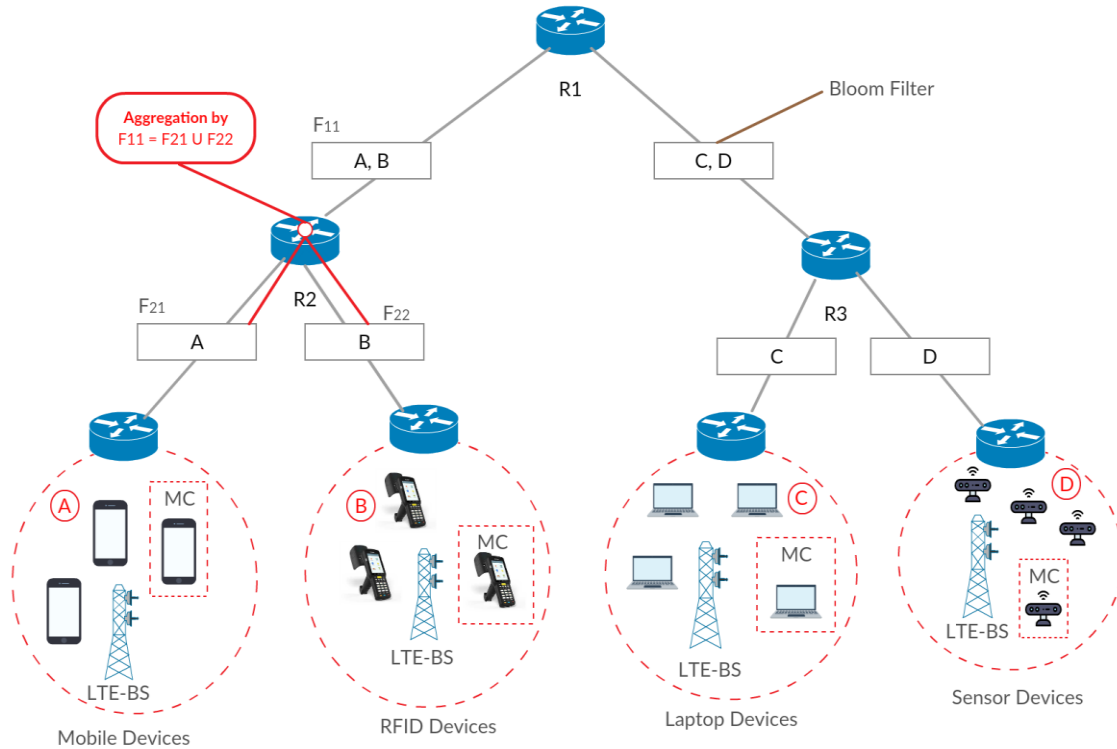


Figure 4. Distributing routers in the sensing area where bloom filters aggregate packets from lower routers and direct them to upper routers.

Every IoT device has its own bloom filter, which includes a pre-defined bit array that represents the current status of the IoT device. In addition, the bloom filter has its own hash function and its length depends on how many parameters can be represented in the bit array. Since IoT devices have limited power resources, increasing the length of the bit array of the bloom filter will expend too much power and deplete the battery's lifetime. Thus, we are proposing a short bit array that is attached to the transmitted packets and mapped into the Bloom filter in order to specify the current context information of the IoT device. We proposed the bit array that has ten bits, as explained in figure 5. In this figure, the first fix bits from the left represent the ID number for the IoT device (e.g. 1 represents the node number 1, 10 represents the node number 2, 1000 represents the node number 8 and etc.). We assume that we have 64 IoT devices in our network. The seventh bit from the left represents the battery lifetime when it is set to 1 (i.e. the remaining battery level is greater than or equal to 70%), the eighth bit from the left represents the battery lifetime when it is set to 1 (i.e. the remaining battery level is greater than or equal to 40% and less than 70%), The ninth bit from the left represents the battery lifetime when it is set to 1 (i.e. the remaining battery level is less than 40%), the tenth bit from the left represents the priority of the packet when it is set to 1 (i.e. urgent packet need to take priority during the transmission mechanism, for instance, some unusual physical phenomena has been detected from the IoT devices). In our design, we proposed only four bits that represent the arrays or parameters that hashed into the bloom filters. If the status of the remaining energy is changed, the bloom filter, have to update and recalculate its own state. This means the bloom filter needs to be updated up

to date for all times for any change that can be occurred in the status of IoT devices. In a different design, various parameters can be inserted into the bit arrays to give an accurate explanation of the status of IoT devices. For example, the device location, the type of device either mobile or static, the operating system and etc.

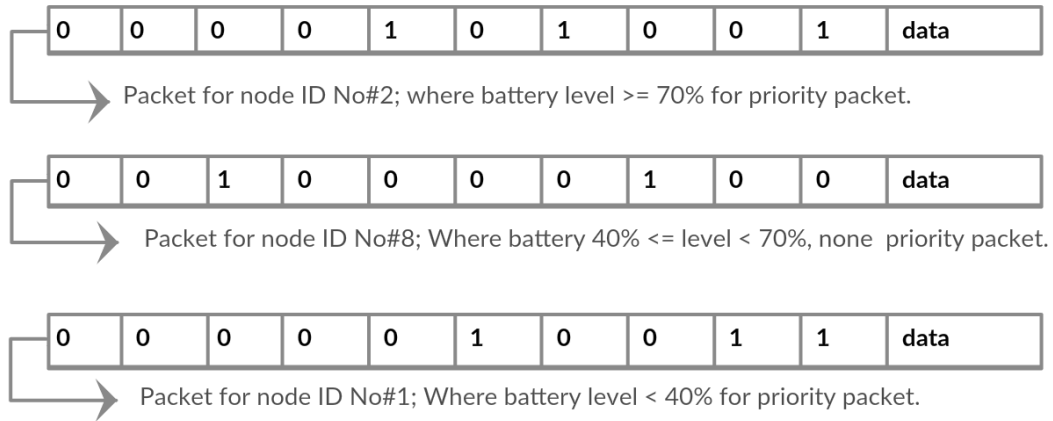


Figure 5. Examples for the proposed bit arrays which are mapped into the Bloom Filters.

As shown in figure 4, different IoT devices are connected to the routers that aggregate the context information from all devices that are located in their domains. The question is when IoT devices should send their context information to the connected routers? In our design, we assume the following:

- Two types of IoT devices are distributed in the sensing filed i.e. the static and mobile devices. The static devices are suitable for normal monitoring applications such as static sensors that are fixed in their locations in order to measure the street temperatures. These type of devices need to be able to operate for long periods, and their batteries lifetime need to be extended as much as possible. Mobile devices such as mobile phones or cars have their own rechargeable batteries, and they can be utilized for monitoring applications as well.
- Scenario 1: When the static or mobile device turns on its own antenna for the first time, it should send the related context information to the connected router which is responsible for the communications for its own domain. The static or mobile node sends a status message to the router in order to extract the new bit array for the IoT device. The router checks the first ninth bits of the bit array if it is already registered in the router table, then this case is not applicable, and the router will ignore the status message. If the first five bits didn't register yet in the router table, then the new IoT device is added to the router domain or group. The sixth, seventh and eighth bits of the bit array that indicate the battery level, and the ninth bit that indicates the priority level of a packet are also registered in the router table for the corresponding IoT device which has just joined the router domain.
- Scenario 2: When the bloom filter for the static or mobile node has been updated for any change in the related bits array (parameters). For example, suppose the seventh bit in the bit array has been changed from 1 to 0, the means the battery level is changed below 70%, when the eighth bit in the bit array is changed from 0 to 1, this means the battery level fro that IoT device is decreased to below 70% and it reached to the level that is higher than or equal 40%. This new change in the battery level should be sent to the corresponding router in order to check its own table, and then update the battery level as explained in the status message sent by the IoT device.

- Scenario 3: When the mobile node changes their location and move from one sensing area to another. In other words, when a mobile node enters a new domain where the network is controlled by a new router. Suppose the mobile IoT device moves from one domain to another domain (handover), the signal will be controlled by a new base station, and the router which is responsible for its own domain should keep tracking all IoT devices that enter its domain. Hence, the status messages need to be sent to the router in order to register the joining IoT device with its battery level.

The three cases for sending the status messages to the corresponding router is illustrated in figure 6.

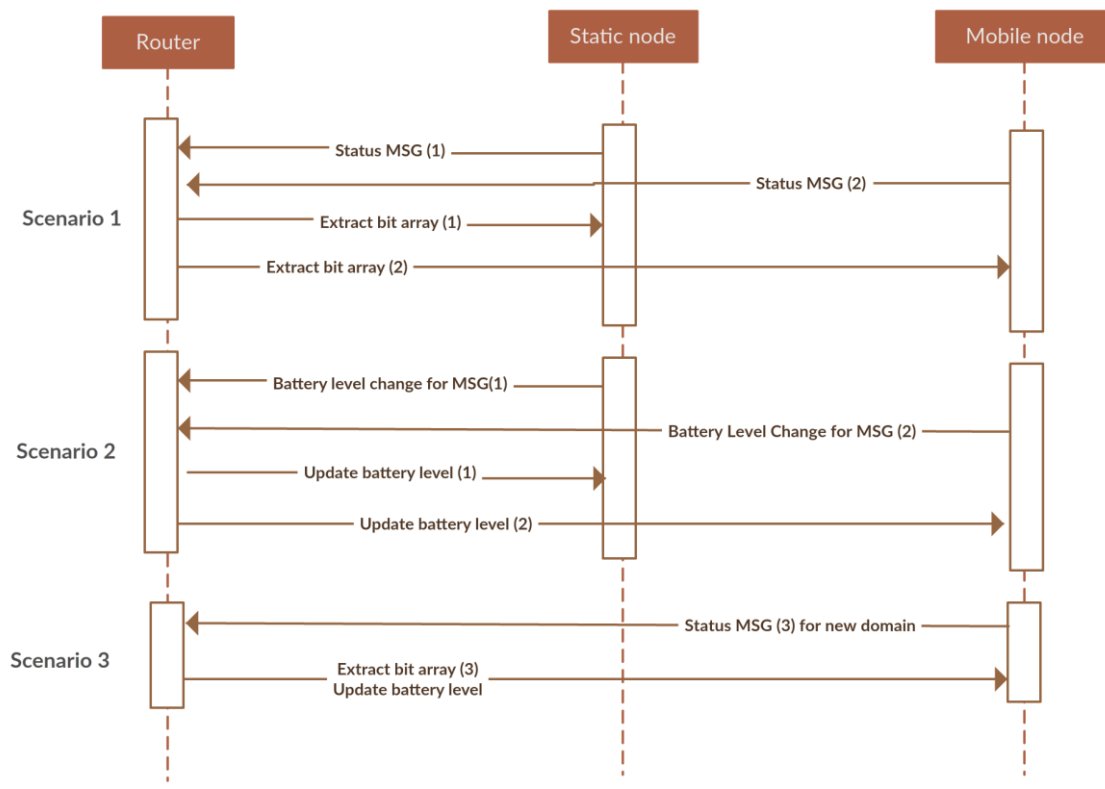


Figure 6. Status message flows between the router and the connected static or mobile IoT devices.

Therefore, the routers will aggregate the context information of connected IoT devices that can be represented in three scenarios, as explained above. The important issue is how to keep the routing process which is based on context-aware information efficient and supports the monitoring applications of IoT. This includes increasing the efficiency of routing information inside each group of IoT devices, or the communication between the IoT devices and the corresponding routers. In addition, another important issue is increasing the accuracy and the efficiency for sharing information between routers that are distributed in the sensing areas or in different parts of the network.

Increasing the efficiency of the routing process is ensured by using the bloom filters in every IoT devices and the corresponding routers since when any change occurred in one context parameters of the IoT devices, the communication messages (status messages) will be sent directly to the upward routers in order to update their router table. If there are no change occurred in the status of the IoT device, it will perform its monitoring operation in a normal way without sending too many status messages to corresponding routers and hence avoid consuming too much power and

resources. The accuracy and efficiency are ensured in the case of the communication between the routers since sending updated messages can be done once any change occurred in one router. The router will send an updated message to all connected routers (wired communication link), and the sending process will continue in point-to-point transmission until the sender (router) receives the acknowledged messages from all connected routers.

For example, in figure 7 we show our network model for the connected routers represents point to point transmission with router 1. Router 1, send updated messages to routers 2,3,4, and 5. Router 2 and 3 send directly their acknowledge messages while because of congestion in round 1, routers 4 and 5 send their acknowledgment messages in round 2. (i.e. In our design we set up the timer for the retransmission process after 10 seconds). This point to point communication mechanism ensures the accuracy for sending updated messages between routers. So, we will ensure that if any update has occurred in any IoT device, all upward routers in the network will be informed by that change in context parameters of that IoT device.

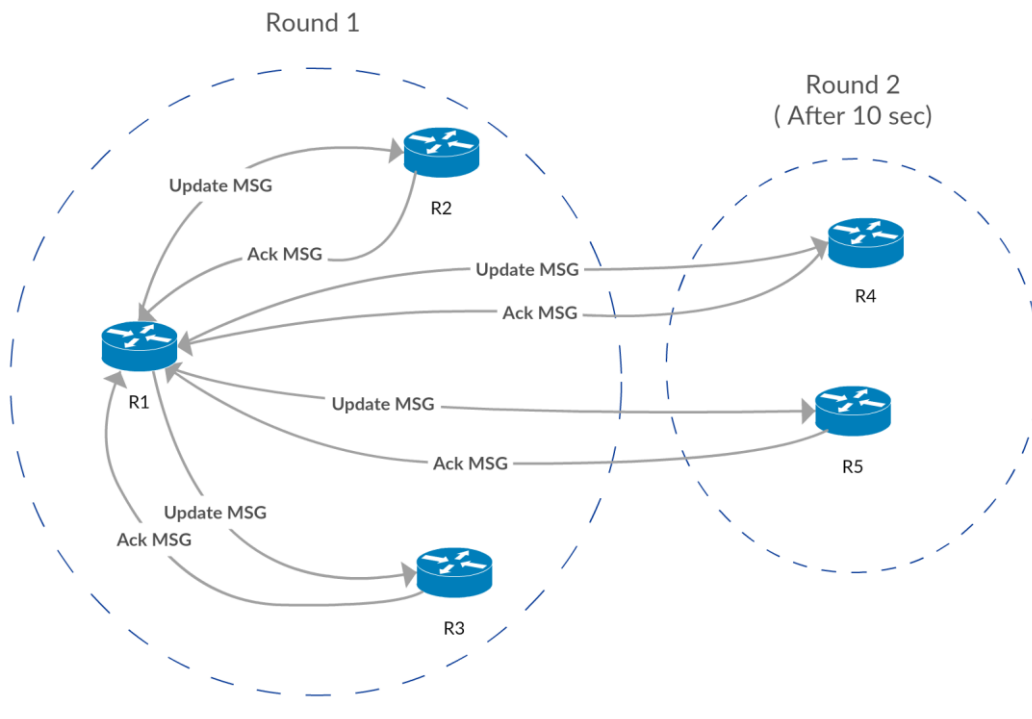


Figure 7. An example for connected routers which form point to point transmission. Router 1 is a sender while routers 2,3,4, and 5 are receivers.

For example, in figure 7 we show our network model for the connected routers in point to point transmission. Router 1, send updated messages to routers 2,3,4 and 5. Router 2 and 3 send directly their acknowledge messages while routers 4 and 5 send their acknowledge messages in round 2 because of the congestion. (i.e. In our design we set up the timer for retransmission process after 10 seconds). This point to point communication mechanism ensures the accuracy for sending updated messages between routers. So, we will ensure that if any update has occurred in any IoT device, all upward routers in the network will be informed by that change in context parameters of that IoT device.

5. EXPERIMENTAL ANALYSIS

In this section, we evaluate our proposed context information aggregation mechanism based on Bloom filters. The simulator utilized to measure the performance metrics is NS-3 which is a simple simulator to draw different scenarios as explained in the following subsection.

5.1. Experimental Scenarios and Parameters

We have two scenarios in our experimental analysis as follows:

- Scenario 1: we distribute 64 sensor nodes in the sensing area for monitoring applications. Four sensor nodes are mobile nodes where they can move from one sensing area (group) to another with variable speeds at different times. The nodes forming 4 groups wherein each group there is only one mobile node at the beginning of the running time of the simulator. Then the mobile nodes move from of group to another. Each group is connected with a router that has a bloom filter in order to collect the routing information from the group members. The lower routers (four routers connected with each other in point to point transmission) are connected to the upper router, which is the final destination for the transmitted packets (figure 8). In real scenarios, this upper router is connected to other routers in different areas of a city or a country for packets to be transmitted to their final destination.
- Scenarios 2,3,4 and 5: similar to scenario 1, but we increase the number of mobile nodes to be 10,18,26 and 40 nodes. These mobile nodes are distributed randomly in the sensing areas (groups). We keep the total number of mobile and static nodes to be 64.

In our simulation, we compare our proposed context information aggregation mechanism based on Bloom filters (CIA-BF) which are based on collecting packets and aggregating them at lower routers, and then sending them to the upper router, we compare it with two routing protocols used in IoT which are Destination Sequenced Distance Vector routing (DSDV), and Ad hoc On-Demand Distance Vector routing (AODV).

For both DSDV and AODV protocols, we keep the number of sensor nodes to be 64 but nodes are distributed randomly in the sensing area where groups of nodes are ignored. So, when a node wants to send a packet it follows the multipath transmission mechanism to deliver the packet to the final destination (the upper router).

In DSDV, a node must build routing tables in the lower routers which include all transmission information for all the nodes in the path between the source node and the upper router or the final destination. The entry of these routing tables needs to be updated periodically [47].

In AODV, routing discovery and maintenance are made periodically when sending packets from the source to the destination. When sending packets the lower routers build the routing table to deliver the packet to the destination on demand [48].

We set up the parameters of our simulation to be as follows:

- The sensing area (i.e. 500m×500m)
- The simulation rounds is 2500 rounds.
- The number of sensor nodes for monitoring applications is 64.
- The number of lower routers is 5.
- The final destination is the upper router (only 1).
- The length of the bit array is 10-bits.

- The packet size is 512 bytes.
- Variable speeds of mobile nodes.
- Three protocols: DSDV, AODV and the proposed CIA-BF.
- Point to point transmission for lower routers.
- For the energy measurements, we assume the Initial energy for a node is 0.4J, the energy consumed by the electronic circuit and radio amplifier of a node are 20nJ/bit and 2 nJ/bit respectively, and the transmission power consumption is 3dBm.
- The performance metrics want to be measured the delay, the packet delay variation (the jitter), the throughput (the number of packets that arrived successfully to the final destination) ,packets dropping ratio and the energy consumption.

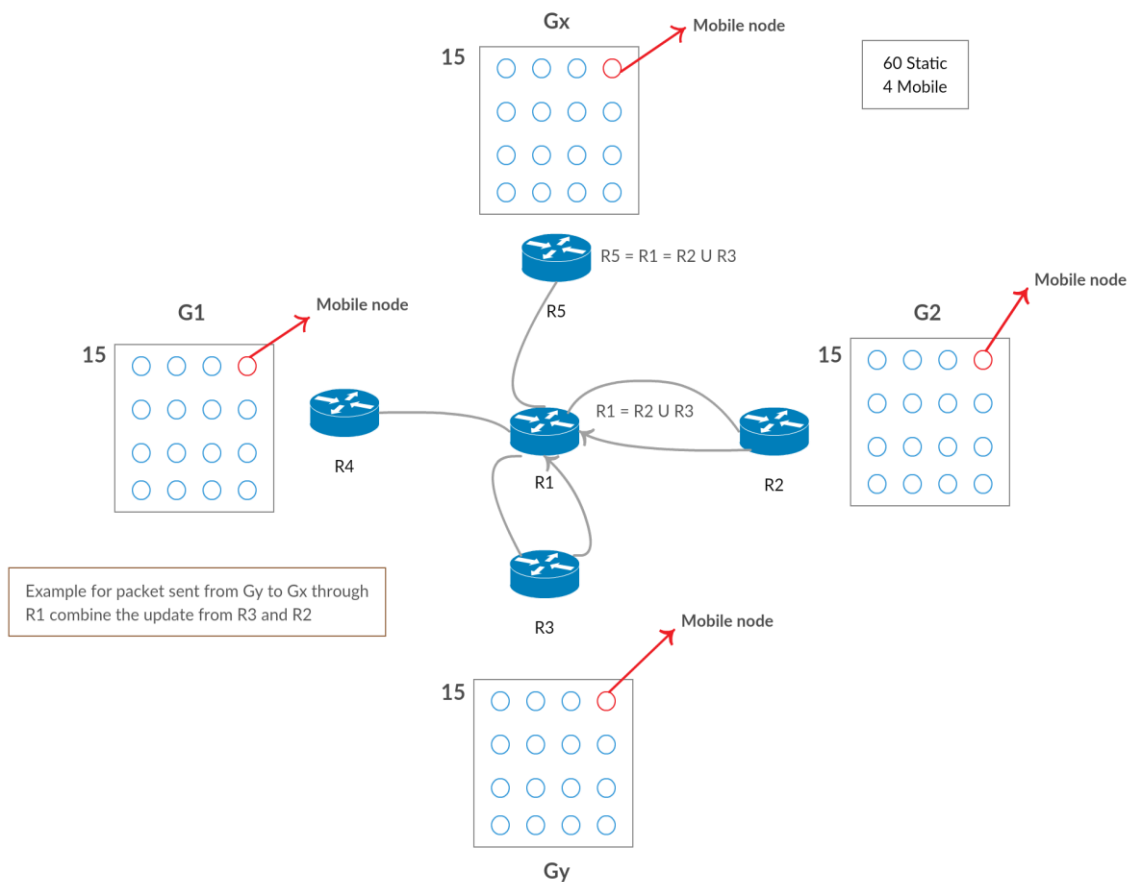


Figure 8. The simulation layout. The upper router (the final destination), the lower routers, the static nodes and the mobile nodes. Static and mobile nodes forming groups. The total number of static and mobile nodes is 64.

5.2. Experimental Results

The first performance metric is the transmission delay which is the time consumed to reach the upper router (the final destination). As shown in figure 9 DSDV protocol has the highest transmission delay when sending packets from a source to the upper router, followed by the AODV protocol. The proposed CIA-BF has the lowest transmission delay, which means the packets can be transferred quickly to the destination even if the number of mobile nodes is increased. However, when going beyond 40 mobile nodes, the transmission delay of our

proposed CIA-BF mechanism is getting closer to the AODV protocol. Let us take as an example when the number of mobile nodes is 18, the transmission delay on the DSDV, AODV and the proposed CIA-BF protocols are 2401, 2212, 1890 milliseconds, respectively. When the number of mobile nodes is 40, the proposed CIA-BF protocol has the transmission delay equal to 1115, which is closer to the AODV protocol (i.e., 1160 milliseconds). The maximum delay (the peak) is reached when the number of mobile nodes is 26, after that, the delay is decreased slowly when increasing the number of mobile nodes for the three simulated protocols.

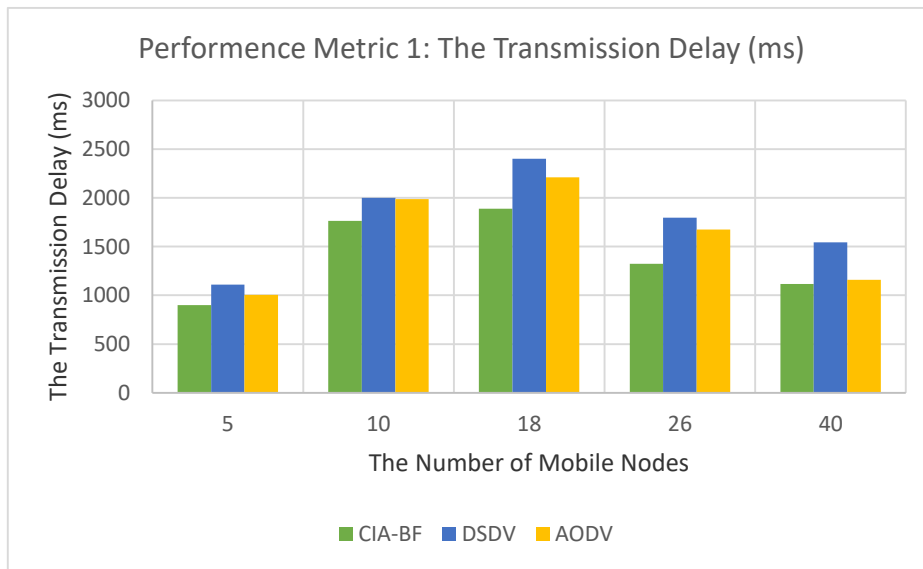


Figure 9. Performance metric 1. The transmission delay vs. the number of mobile nodes

The second performance metric is jitter. As shown in figure 10, the DSDV protocol shows increase in the delay variation gradually as the number of mobile nodes increased. This increase in jitter is expected because of the fact that a node must build routing tables in the lower routers which includes all transmission information periodically which affects packets transmission. Whereas the jitter reaches its maximum peak point in AODV protocol when the number of mobile nodes is 26, then the jitter decreased to lower values. At point 26, the maximum delay reached 643 milliseconds. In the proposed CIA-BF protocol, the jitter is fluctuating. However, it stills lower than both the DSDV and AODV protocols. Hence, the packet delay variation in CIA-BF is much better than the other protocols even if the number of mobile nodes is increased. The fluctuating curve will continue, and this curve is lower than the curves of the DSDV and AODV protocols. For example, when the number of mobile nodes is 26, the packet delay variations for the three protocols are 754, 643, and 343 milliseconds, respectively.

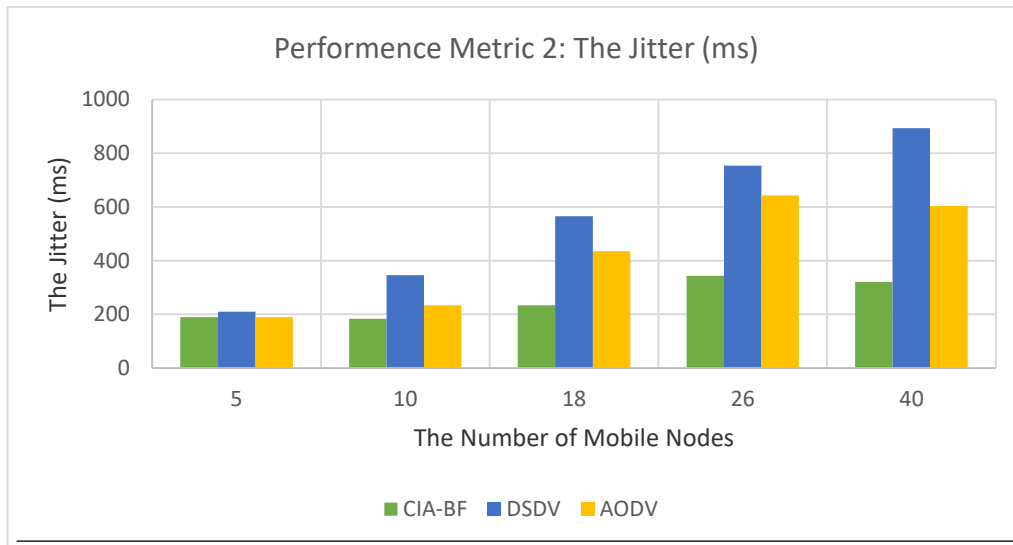


Figure 10. Performance metric 2. The jitter vs. the number of mobile nodes

The third performance metric is the throughput or the number of packets that arrived successfully at the upper router. As shown in figure 11, the number of packets that arrived at the final destination when the DSDV protocol is simulated is 234, 454, 765, 985, and 1003 when the mobile nodes are 5, 10, 18, 26, and 40, respectively. This throughput is very close to the AODV protocol (i.e., 300, 489, 801, 990, and 1019 packets). Whereas, the number of successfully arrived packets in the proposed CIA-BF protocol is higher (i.e., 340, 645, 843, 1134, and 1565 packets). This shows how the performance of the proposed protocol is efficient in comparison with the two protocols. Aggregating packets at lower routers and sending them directly to the upper routers shows remarkable results in the number of the packet that arrived successfully to the final destination.

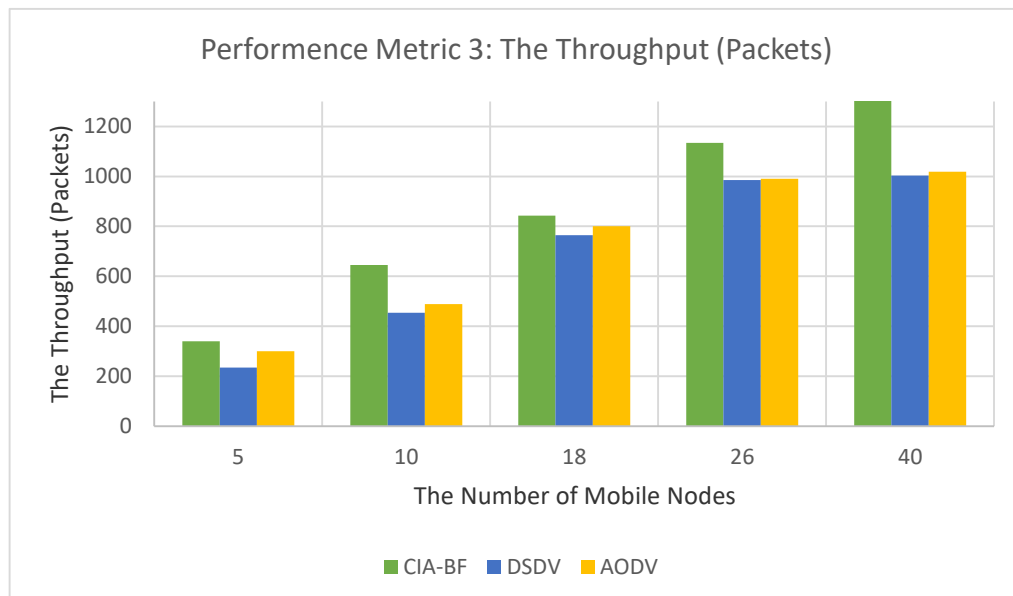


Figure 11. Performance metric 3. The throughput vs. .the number of mobile nodes

The fourth performance metric is the packets dropping ratio, which is an important metric to determine the performance of the proposed CIA-BF protocol. In figure 12, the percentages of

packet dropping ratio in CIA-BF protocol reach its maximum point when the number of the mobile nodes is 40 (i.e., 54%) while it is reached 78 % in DSDV protocol and 66% in AODV protocol at the same number of mobile nodes. The figure shows how the percentages of dropping packets increase gradually when increasing the number of mobile nodes. Context-aware aggregation mechanism in CIA-BF plays a very important role to correctly identify packets and successfully deliver them to the final destination in comparison with DSDV and AODV protocols.

The fifth performance metric is energy consumption. Here, we compare our proposed CIA-BF mechanism with both DSDV and AODV protocols. In CIA-BF, when a node wants to send a packet, it follows the shortest path at the lower routers, and the packet will continue to follow the shortest path until it arrives to the final destination (the upper router). Because that in the CIA-BF mechanism the nodes are grouped into five groups, this will facilitate the delivery of packets that have the highest energy level as illustrated in the ten bits arrays that are attached in the header of the packets as explained earlier. Another parameter in the ten-bit arrays is the priority of a packet when it is set to 1, which means that a specific node that has the highest priority packet needs to be delivered quickly to the destination. The DSDV and AODV protocols follow a multipath transmission scenario where a packet needs to be transmitted to the final destination through multi-hops (nodes) which consume too much energy. In our simulation, we use the first order radio model [49] to measure energy consumption.

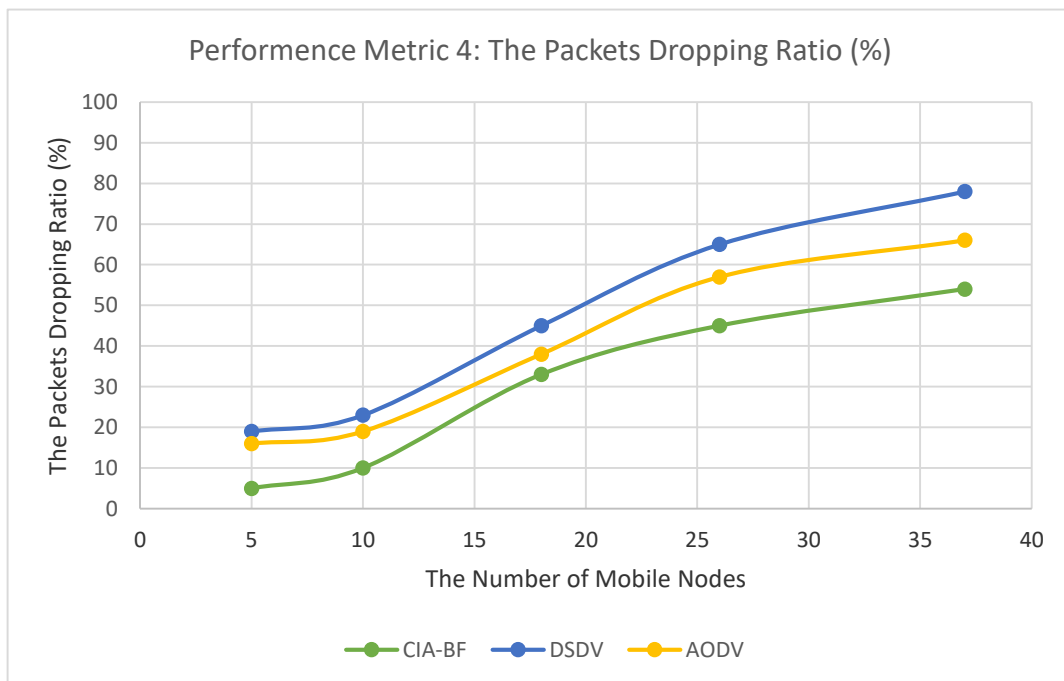


Figure 12. Performance metric 4. The packet-dropping ratio vs. the number of mobile nodes

As shown in figure 13, our proposed CIA-BF mechanism outperforms both DSDV and AODV protocols in terms of energy consumption which demonstrates effective packet delivery because of using the bit arrays that represent the battery level of the source of transmission.

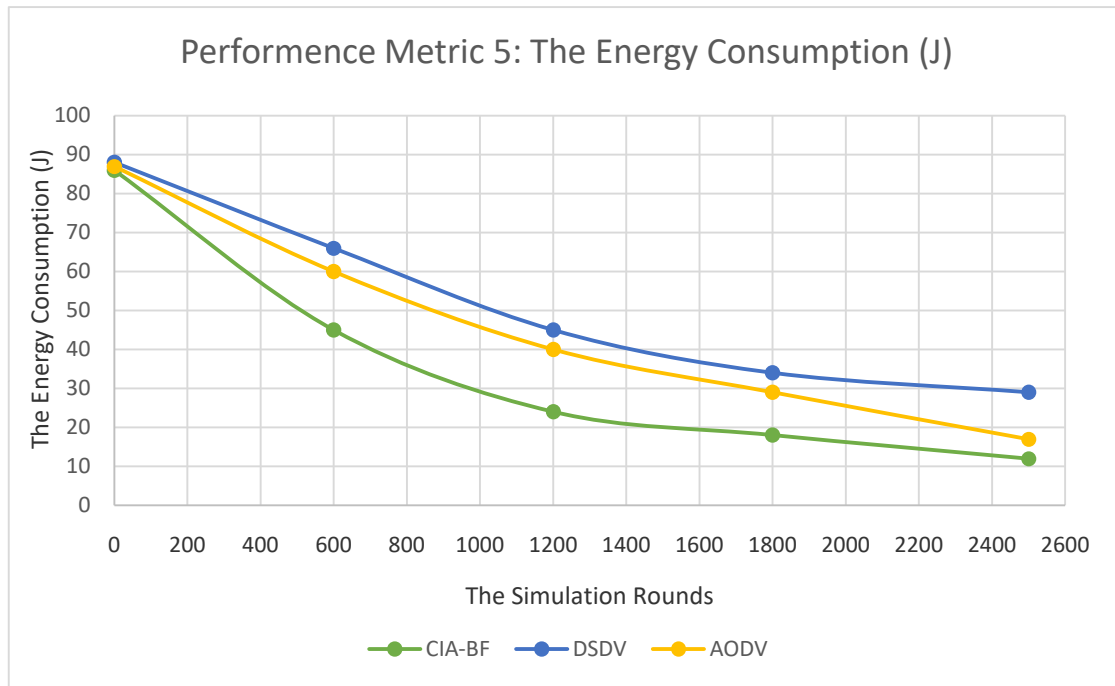


Figure 13. Performance metric 5. The energy consumption vs. the simulation rounds

6. CONCLUSION

In this paper, we proposed the context information aggregation mechanism based on bloom filter for fast packet delivery in IoT. In our mechanism bloom filters are included in all sensor nodes to collect routing information. Lower routers are distributed in the sensing area to aggregate packets and deliver them hierarchically to the final destination (the upper router). The sensor nodes are grouped in many clusters, and the packets are attached with a 10-bits array that determine the energy level of the source nodes and the priority of the transmitted packet. In other words, we reduce the size of routing information using the aggregation mechanism which is based on connecting each group of sensor nodes with lower routers which are connected to the final destination after operating their bloom filters. Our simulation results show a significant improvement in the IoT performance metrics such as packets transmission delay, jitter, the throughput, packets dropping ratio, and the energy consumption in comparison with Destination DSDV and AODV protocols.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

- [1] D. Arellanes and K. Lau, Evaluating IoT service composition mechanisms for the scalability of IoT systems, *Future Generation Computer Systems*, 2020, pp. 827-848.
- [2] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed and M. Imran, Securing IoTs in distributed blockchain: Analysis, requirements and open issues, *Future Generation Computing Systems*, 2019, pp. 325-343.

- [3] F.X. Ming, R.A.A. Habeeb, F.H.B. Md Nasaruddin and A.B. Gani, Real-time carbon dioxide monitoring based on IoT & cloud technologies, Proceedings of the 2019 8th International Conference on Software and Computer Applications (ACM), 2019, pp. 517-521.
- [4] Cisco Visual Networking Index: Forecast and Trends, 2018/2023, White Paper.
- [5] K. Kumar and S. Kumar, Energy efficient link stable routing in Internet of Things, International Journal of Information Technology, 2018, pp. 465-479.
- [6] S. Johansson, Tackling the IoT opportunity for commercial lines insurance, 2019, <https://www.mckinsey.com/industries/financial-services/our-insights/tackling-the-iot-opportunity-for-commercial-lines-insurance>
- [7] K. Ashton, That 'Internet of Things' thing, RFID Journal, 2009.
- [8] M. Weiser, The computer for the 21st century, Scientific American, 1991, pp. 94-105.
- [9] International Telecommunication Union (ITU-T), Overview of the Internet of Things, Technical Report ITU-T Y.4000/Y.2060, 2012.
- [10] Y. Wang, Y. Tian, R. Miao and W. Chen, Heterogeneous IoTs routing strategy based on cellular address, IEEE International Conference on Smart Internet of Things (SmartIoT), 2018, pp. 64-69.
- [11] A. Dhumane, R. Prasad and J. Prasad, Routing issues in Internet of Things: A survey, Proceedings of the International MultiConference of Engineers and Computer Scientists Vol. I (IMECS:2016), 2016, pp. 16-18.
- [12] A. Aadri and N. Idrissi, An energy efficient hierarchical routing scheme for wireless sensor networks, Computer Science & Information Technology, 2017, pp. 137-148.
- [13] D. Airehrour, J. Gutierrez and S.K. Ray, Secure routing for Internet of Things: A survey, Journal of Network Computers and Applications, 2016, pp. 198-213.
- [14] D. Dragomir, L. Gheorghe, S. Costea and A. Radovici, A survey on secure communication protocols for IoT systems, In Proceedings of the 2016 International Workshop on Secure Internet of Things (SIoT'16), 2016, 47 -62.
- [15] L. Anh Tuan, J. Loo, A. Lasebae, A. Vinel, C. Yue and M. Chai, The impact of rank attack on network topology of routing protocol for low-power and lossy networks, IEEE Sensors Journal, 2013, pp. 3685-3692.
- [16] C. Sharma and D.N.K. Gondhi, Communication protocol stack for constrained IoT systems, IEEE 3rd International Conference on Internet of Thing: Smart Innovation and Usage (IoT-SIU), 2018, pp. 1-6.
- [17] T. Chang, T. Watteyne, B. Wheeler, F. Maksimovic, O. Khan, S. Mesri, L. Lee, I. Suci, I. D. Burnett, X. Vilajosana and K. Pister, 6TiSCH on SCμM: Running a synchronized protocol stack without crystals, *Sensors*, 2020, pp. E1912.
- [18] A. Dhumane, R. Prasad and J. Prasad, Routing issues in Internet of Things: A survey, Proceedings of the International MultiConference of Engineers and Computer Scientists, 2016, pp. 16-18.
- [19] G. Abowd, A. Dey, P. Brown, N. Davies, M. Smith and P. Steggles, Towards a better understanding of context and context-awareness, *Handheld and Ubiquitous Computing*, 1999, pp. 304-307.
- [20] C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, Context aware computing for the Internet of Things: A survey, IEEE Communications Surveys Tutorials, 2014, pp. 414-454.
- [21] C. Perera, C.H. Liu, S. Jayawardena and M. Chen, A survey on Internet of Things from industrial market perspective, IEEE Access, 2014, pp. 1660-1679.
- [22] R.K. Poluru and S. Naseera, A literature review on routing strategy in the Internet of Things, Journal of Engineering Science and Technology Review, 2017, pp. 50-60.
- [23] V.B. Carvalho, Including context in a routing algorithm for the Internet of Things, Ph.D. dissertation, Dept. de Engenharia Informatica, Universidade Nova de Lisboa, Lisbon, Portugal, 2010
- [24] S. Mayer, D. Guinard and V. Trifa, Searching in a web-based infrastructure for smart things, 3rd IEEE International Conference on the Internet of Things, 2012, pp. 119-126.
- [25] G.S. Prasad, P. Kaliyar, M. Conti, P. Tiwari, V.B.S. Prasath, D. Gupta and A. Khanna, 2197 LISA: Lightweight context-aware IoT service architecture. *Journal of Cleaner Production*, 2019, pp. 1345-1356.
- [26] P. Shankar, V. Ganapathy and L. Iftode, Privately querying location-based services with Sybilquery, 2009, pp. 31e40.
- [27] IEEE Standard for Local and Metropolitan Area Networks, Part 21: Media Independent Handover, IEEE Std 802.21-2008, 2009, pp. c1-301.

- [28] N. Saeed, M. Abbod and H. Al-Raweshidy, Intelligent MANET routing system, 22nd International Conference on Advanced Information Networking and Applications – Workshops, 2008, pp. 1260-1265
- [29] N. Shah and D. Qian, Context-aware routing for peer-to-peer network on MANETs, IEEE International Conference on Networking, Architecture, and Storage, 2009, pp. 135- 139.
- [30] Z. Zhao, T. Braun, D. Rosário and E. Cerqueira, CAOR: Context-aware adaptive opportunistic routing in mobile ad-hoc networks, 7th IFIP Wireless and Mobile Networking Conference (WMNC), 2014, pp. 1-8.
- [31] E.C.R. de Oliveira, E.F. Silva, D.G. Passos, J.F. Naves, D.C. Muchaluat-Saade, I.M. Moraes and C. Albuquerque, Context-aware routing in delay and disruption tolerant networks, International Journal of Wireless Information Networks, 2016, pp. 231-245.
- [32] B.B. Bista and D.B. Rawat, Ea-PRoPHET: An energy aware PRoPHET-based routing protocol for delay tolerant networks, IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), 2017, pp. 670-677.
- [33] E. Rosas, F. Grary and N. Hidalgo, Context-aware self-adaptive routing for delay tolerant network in disaster scenarios, Ad Hoc Networks Journal, 2020, pp. 102095.
- [34] Y. Chen, J.P. Chanet, K.M. Hou, H. Shi and G. de Sousa, A scalable context-aware objective function (SCAOF) of routing protocol for agricultural low-power and lossy networks (RPAL), Sensors, 2015, pp. 19507-19540.
- [35] Y. Saied, A. Olivereau, D. Zeglache, M. Laurent, Trust management system design for the internet of things: a context-aware and multi-service approach, Computr & Security. 39 (2013) 351–365.
- [36] S. Taghizadeh, H. Bobarshad and H. Elbiaze, CLRPL: Context-aware and load balancing RPL for IoT networks under heavy and highly dynamic load, IEEE Access, 2018, pp. 23277-23291.
- [37] I. Kertiou, S. Benharzallah, L. Kahloul, M. Beggas, R. Euler, A. Laouid and A. Bounceur, A dynamic skyline technique for a context-aware selection of the best sensors in an IoT architecture, Ad Hoc Networks, 2018, pp. 183-196.
- [38] H.D.S. Raujo, R.H. Filho, J.J.P.C. Rodrigues, R.D.A.L Rabelo, N.D.C. Sousa, J.C.C.L.S. Filho and J.V.V. Sobral, A proposal for IoT dynamic routes selection based on contextual information, Sensors, 2018, p. 353.
- [39] N.C. Sousa, J.V.V. Sobral, J.J.P.C. Rodrigues, R.A.L. Rabelo and P. Solic, ERAOF: A new RPL protocol objective function for Internet of Things applications, Proceedings of the 2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech), 2017, pp. 1-5.
- [40] A. Singh, S. Garg, S. Batra, N. Kumar and J.J. Rodrigues, Bloom filter based optimization scheme for massive data handling in IoT environment, Future Generation Computing Systems, 2018, pp. 440-449.
- [41] B.H. Bloom, Space/time trade-offs in hash coding with allowable errors, Communications of the ACM, 1970, pp. 422-426.
- [42] A. Broder and M. Mitzenmacher, Network applications of Bloom filters: A survey, Internet Mathematics, 2004, pp. 485-509.
- [43] A.Z. Broder and M. Mitzenmacher, Network applications of Bloom filters: A survey, Internet Mathematics, 2005, pp. 485-509.
- [44] L. Luo, D. Guo, R.T.B. Ma, O. Rottenstreich and X. Luo, Optimizing Bloom filter: Challenges, solutions, and comparisons, IEEE Communications Surveys Tutorials, 2019, pp. 1912-1949.
- [45] A. Alrawais, A. Alhothaily, C. Hu and X. Cheng, Fog computing for the Internet of Things: Security and privacy issues, IEEE Internet Computing, 2017, pp. 34-42.
- [46] M. Amoretti, O. Alphand, G. Ferrari, F. Rousseau and A. Duda, DINAS: A lightweight and efficient distributed naming service for All-IP wireless sensor networks, IEEE Internet of Things Journal, 2017, pp. 670-684.
- [47] C. E. Perkins and P. Bhagwat, “Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers,”ACM SIGCOMM Comput. Commun. Rev., vol. 24, no. 4, pp. 234–244, 1994.
- [48] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing,” 2003.

- [49] A. Ahmad, N. Javaid, M. Imran, M. Guizani and A. A. Alhamed, "An Advanced Energy Consumption Model for terrestrial Wireless Sensor Networks," 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), Paphos, 2016, pp. 790-793.

AUTHORS

Fawaz Alassery received his M.E. in telecommunication engineering from the University of Melbourne, Australia. He also received his Ph.D. degree in Electrical and Computer Engineering from Stevens Institute of Technology, Hoboken, New Jersey, USA. Nowadays, Alassery is working as an associate professor and the dean of E-learning and Information Technology at Taif University in Saudi Arabia. His research interests include the energy-efficient design of Smart WSNs and the network design of the Internet of Things (IoT).



Maha M. Althobaiti is an assistant professor in the Department of Computer Science at Taif University, Taif, Saudi Arabia. Ms. Maha obtained her Ph.D. degree in Computer Science in 2016 from the University of East Anglia, United Kingdom. She is working as the Vice Dean of Information Technology and her research interests include Network Security, IoT, Data Mining, HCI, and Usable Security.