International Journal of Engineering Research and General Science Volume 3, Issue 4, July-August, 2015
ISSN 2091-2730

EFFICIENT DATA COLLECTION FOR LARGE SCALE MOBILE MONITORING APPLICATION

Karthikeyan.v[1]

[1]ECE, Angel College of Engineering & Technology,

Tirupur, 641606, India

Karthik.v.1987@gmail.com

Abstract-Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSNs) have been popular in the industrial field and both have undergone dramatic development. RFID and WSNs are well-known for their abilities in identity identification and data transmission, respectively, and hence widely used in applications for health monitoring. Though the integration of a sensor and an RFID tag was proposed together both RFID tag and sensed information to enhance the performance of the applications. The concept has been implied Hybrid RFID and WSN system (HRW) that synergistically integrates the traditional RFID system and WSN system for efficient data collection. HRW has hybrid smart nodes that combine the function of RFID tags, the reduced function of RFID readers and wireless sensors. The proposed method improves data transmission efficiency and protects data privacy and avoids malicious data selective forwarding in data transmission. The effectiveness of the proposed method improves the performance of HRW in terms of the cost of deployment, transmission delay capability, and tag capacity requirement.

Keywords— Radio Frequency Identification, Wireless Sensor Networks, Hybrid RFID and WSN

INTRODUCTION

A wireless sensor network consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, and to cooperatively pass their data through the network to main location. The more modern networks are bi-directional, also enabling control of sensor activity

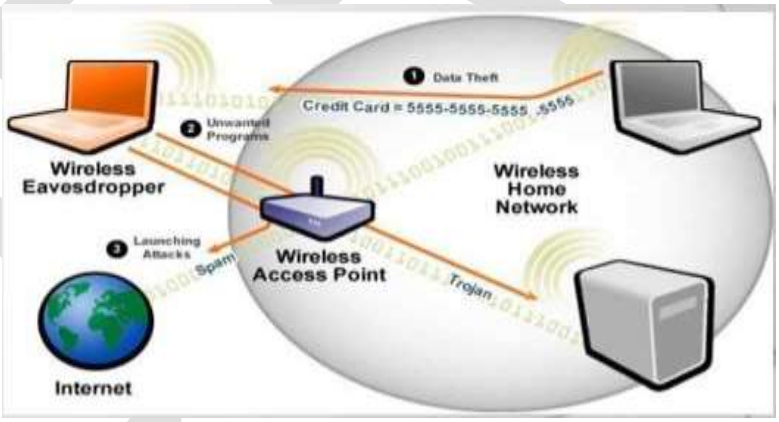


Figure 1 Wireless sensor network

The system consists of smart node, which combines the function of RFID and Wireless sensor network. By implementing this smart node the process time is reduced. This model includes various mechanisms such as Hybrid RFID and WSN, Data privacy and Manipulation, Cryptographic key, Hash function, Cipher text & Trace driven

LITERATURE SURVEY

Exploiting Reactive Mobility for Collaborative Target Detection in Wireless Sensor Networks [12] exploits reactive mobility to improve the target detection performance of wireless sensor networks. In this approach, mobile Sensors collaborate with static sensors and move reactively to achieve the required detection performance. Specifically, mobile sensors initially remain stationary and are directed to move toward a possible target only when a detection consensus is reached by a group of sensors. The accuracy of final

detection result is then improved as the measurements of mobile sensors have higher Signal-to-Noise Ratios after the movement. They develop a sensor movement scheduling algorithm that achieves near-optimal system detection performance under a given detection delay bound. Energy-Efficient Transmission for Wireless Energy Harvesting Nodes [10] implies, the best data transmission strategy is found for a finite battery capacity WHEN that has to fulfill some Quality of Service (QoS) constraints, as well as the energy and data causality constraints. As a result, it can state that losing energy due to overflows of the battery is inefficient unless there is no more data to transmit and that the problem may not have a feasible solution. Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks[3] implies the two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. It shows the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols.

ALBA-R: Load-Balancing Geographic Routing around Connectivity Holes in Wireless Sensor Networks [2] implies ALBA-R, a protocol for *converge casting* wireless sensor networks. ALBA-R features the cross-layer integration of geographic routing with contention-based MAC for relay selection and load balancing (ALBA) as well as a mechanism to detect and route around connectivity holes (Rainbow). ALBA and Rainbow (ALBA-R) together solve the problem of routing around a dead end without overhead-intensive techniques such as graph planarization and face routing. The protocol is localized and distributed, and adapts efficiently to varying traffic and node deployment.EMBA: An Efficient Multihop Broadcast Protocol for Asynchronous Duty-Cycled Wireless Sensor Networks [6] proposed an efficient Multihop broadcast protocol for asynchronous duty-cycled wireless sensor networks (EMBA) where each node independently wakes up according to its own schedule. EMBA adopts two techniques of the forwarder's guidance and the overhearing of broadcast messages and ACKs. A node transmits broadcast messages with Guidance to neighbor nodes. The guidance presents how the node forwards the broadcast message to neighbor nodes by using unicast transmissions. This technique significantly reduces redundant transmissions and collisions. The overhearing of broadcast messages and ACKs helps to reduce the number of transmissions, thus it minimizes the active time of nodes. Transmission Efficient Clustering Method for Wireless Sensor Networks using Compressive Sensing [11] implies a clustering method that uses hybrid CS for sensor networks. The sensor nodes are organized into clusters. Within a cluster, nodes transmit data to cluster head (CH) without using CS. CHs use CS to transmit data to sink. At first propose an analytical model that studies the relationship between the size of clusters and number of transmissions in the hybrid CS method, aiming at finding the optimal size of clusters that can lead to minimum number of transmission.

Mobility based Energy Efficient and Multi-Sink Algorithms for Consumer Home Networks [9] implies fast development of the Internet, wireless Communications and semiconductor devices, home networking has received significant attention. Consumer products can collect and transmit various types of data in the home environment. Typical consumer sensors are often equipped with tiny, irreplaceable batteries and it therefore of the utmost importance to design energy efficient algorithms to prolong the home network lifetime and reduce devices going to landfill. Sink mobility is an important technique to improve home network performance including energy consumption, lifetime and end-to-end delay. Also, it can largely mitigate the hot spots near the sink node. The selection of optimal moving trajectory for sink node(s) is an NP-hard problem jointly optimizing routing algorithms with the mobile sink moving strategy is a significant and challenging research issue. The influence of multiple static sinks nodes on Energy consumption under different scale networks is first studied and an Energy-efficient Multi-sink Clustering Algorithm (EMCA) is proposed and tested.QOF: Towards Comprehensive Path Quality Measurement in Wireless Sensor Networks [8] explains the Quality of Forwarding, a new metric which explores the performance in the gray zone inside a node left unattended in previous studies. By combining the QOF measurements within a node and over a link, it is able to comprehensively measure the intact path quality in designing efficient multi-hop routing protocols. By implementing QoF and build a modified Collection Tree Protocol (CTP).

Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks [7] implies a scalable authentication scheme based on elliptic curve cryptography (ECC). While enabling intermediate nodes authentication, our proposed scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. In addition, our scheme can also provide message source privacy. Exact and Heuristic Algorithms for Data-Gathering Cluster-Based Wireless Sensor Network Design Problem [5] implies an integrated topology control and routing problem in cluster-based WSNs. To prolong network Lifetime via efficient use of the limited energy at the sensors, adopt a hierarchical network structure with multiple sinks at which the data collected by the sensors are gathered through the cluster heads (CHs). This method considers a mixed-integer linear programming (MILP) model to optimally determine the sink and CH locations as Well as the data flow in the network. Our model effectively utilizes both the position and the energy-level aspects of the sensors while selecting the CHs and avoids the highest-energy sensors or the sensors that are well-positioned sensors with respect to sinks being selected as CHs repeatedly in successive periods. For the solution of the MILP model, it develops an effective Benders decomposition (BD) approach that incorporates an upper bound heuristic algorithm, strengthened cuts, and an -optimal framework for accelerated convergence.

MECHANISM

After smart node *A* collects the sensed data, it appends the sensed data with a timestamp and stores the data in its tag through RFRR. Figure 3 shows an example of data collection process of two smart nodes. After the sensor unit in a smart node collects the information about its tag host (Step 1), it asks RFRR to store the information into its tag (Step 2). Once two nodes move into the transmission range of each other, the RFRR in a node reads the information stored in another node's tag (Step 3). Based on the host ID and time-stamp, the node checks if it has stored the information previously. If not, the RFRR then stores the acquired information into the local tag (Step 4).

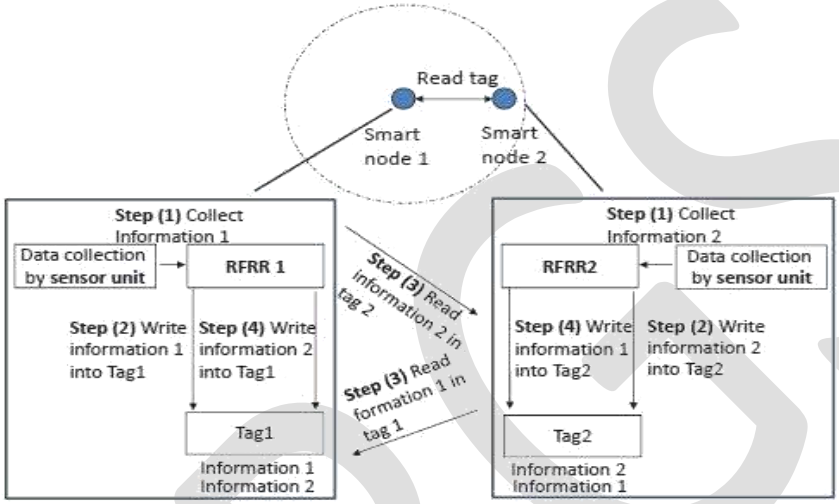


Figure 2 The replication process of two smart nodes

REDUCING REPLICATE DATA

When a node enters the reading range of an RFID reader, the RFID reader reads the information in the node's tag. If several nodes enter the range of RFID reader at the same time, the RFID reader gives the first meeting tag the highest priority to access the channel, reducing channel Contention and long distance transmission interference. The RFID reader can erase the information in the tag after obtaining it. With this data transmission, after an RFID reader receives the information of a node, many nodes still hold the replicas of the information. Exchanging such delivered and redundant information incurs high transmission overhead but does not contribute to information collection. In order to reduce the unnecessary message transmission, we use a tag clean-up algorithm to delete the delivered messages in the system. Specifically, after an RFID reader reads the information from a node, the reader sends the node a directory containing the tag IDs and timestamps of recently received data items. This directory has a TTL (Time to live) with it. It is then broadcasted among nodes and will be deleted when TTL expires. After receiving the directory, the nodes delete the delivered information in their own tags. Considering that the timestamp and ID of each information item have much less size than a complete data item, the overhead of the directory broadcasting is small.

CLUSTER BASED DATA TRANSMISSION

Replicating data between any two encountered smart nodes generates a high cost. Concurrent data transmission from many nodes to an RFID reader causes channel access congestion. Also, it is not easy to erase Duplicate data that is already reported to the RFID readers from replica nodes. We propose enhanced data transmission algorithms to mitigate these problems. A simple algorithm to reduce the cost is to enable a source node to replicate its data to a limited number of nodes. Here, we describe two enhanced algorithms called cluster-member based and cluster-head algorithms, in which smart nodes are clustered to different virtual clusters and each cluster has a cluster head. In the cluster-member based algorithm, cluster members replicate their tag data between each other. When a cluster member of a virtual cluster enters the reading range of an RFID reader, by reading the aggregated tag information from the cluster member, the RFID reader receives all information of nodes in this virtual cluster. In the cluster-head based algorithm, cluster members replicate their tag data to the cluster head. When a cluster head of a virtual cluster reaches an RFID reader, the RFID reader receives all information of nodes in this virtual cluster. This enhanced method greatly reduces channel access congestion, reduces the information exchanges between nodes and makes it easy to erase duplicate information in a cluster. To form the clusters in the cluster-member based algorithm, nodes report their encountering frequency to the server through the RFID readers. The server forms nodes with high encountering frequency into a cluster and notifies the cluster nodes through the RFID readers. The cluster head for a cluster can be selected in a number of ways depending on the application requirement. For example, in a health

monitoring application where real-time data collection is required, the nodes with the most contact frequency with cluster members and RFID readers should be the cluster heads. In the supply chain where nodes are always close to each other, the nodes with the highest energy should be the cluster heads. The former example to show how to choose cluster heads. Algorithm 3 shows the pseudo code of cluster head determination and data transmission conducted by each smart node in the second algorithm. RFID readers record the meeting frequency with each node and report the data to the back-end server. The server calculates the sum of the frequencies from different readers for each node *j*, denoted by *frj* and selects *N* nodes with the highest *frj* as the cluster heads. The information of the selected cluster heads along with their *fr* is transmitted back to the RFID readers, which will forward the information to the nodes. We use *fnij* to denote the meeting frequency between nodes *i* and a cluster head *j*. A node measures its *fnij* frj* for each cluster head candidate, and selects the one with the highest metric as its cluster head. The metric of *fnij* frj* indicates how fast cluster head *j* can forward node *i*'s data to an RFID reader. Through RFID readers, each node reports its selected cluster head to the server and the server then notifies all heads about their cluster members. The head determination can also be solely conducted at the server to reduce the communication. As a result, each cluster head is associated with a group of nodes, and it can most quickly forward the data to RFID readers for its cluster members.

In the HRW system, since the data is stored in tags, active nodes can retrieve the information at any time from a sleeping node. In traditional WSNs, however, nodes in sleeping mode cannot conduct data transmission. Therefore, the HRW system can greatly improve packet transmission efficiency with the RFID technology.

COMMUNICATION SECURITY MECHANISMS

The multi-hop message transmission mode in HRW improves the communication efficiency. However, such method introduces privacy and security risks. Low-cost RFID nodes are not tamper-resistant and deployed in open environment, thus the attackers can easily physically access and take control of these nodes. The attacker can obtain all the information in the compromised nodes and use the compromised nodes to obtain sensitive information and disrupt system functions. Thus, in this section, we consider two security threats arising from node compromise attacks: data manipulation and data selective forwarding.

DATA PRIVACY AND MANIPULATING

In the system, each smart node replicates its information to other nodes. Once a node is compromised, all the information of other nodes is exposed to the adversaries, which is dangerous especially in privacy sensitive applications such as health monitoring. A malicious node can also manipulate the gathered information and provide false information to the readers. Therefore, it is important to protect the confidentiality and authenticity of tag information in data transmission. Public key operations are too expensive for the smart nodes due to their limited computing, storage and bandwidth resources. Then it develops a symmetric key based security scheme in our system. In this model, it focuses on the threats due to the compromised smart nodes and assumes the readers are secure. In our security Scheme, each smart node *N* is initially assigned with an individual key *KN*. The pairs (*N, KN*) of all smart nodes are stored in a central server, which can be securely accessed by the readers. To achieve data confidentiality, each smart node *N* generates a temporary key $K\_N = H(Nonce|KN)$, where *Nonce* is a nonce number which can be the timestamp of RFID data, *H* (*) is a system-wide secure hash function known by every node, and" |" represents the concatenation of two strings. Node *N* uses this symmetric key to encrypt its data *DN* and sends the encrypted data, denoted by *En* (*K_N, DN*), to other nodes. The use of temporary keys for every data transmission further enhances the security against the cipher text-only attacks by interpreting historical transmissions. To protect data authenticity, node *N* also computes the message authentication code with the temporary key *K_ N*, denoted by *MAC* (*K_ N, N|DN*). The message from a smart node is in the format of (*N, Nonce, En* (*K_ N, DN*)*, MAC* (*K _ N, N|DN*)). The procedure of data reading with encryption and authentication. When a reader receives the data, it first sends to the central server the tag ID *N* and *Nonce*. The server finds *KN* and computes the temporary key *K_ N*, and then securely sends *K_N* to the reader. After receiving *K_N*, the reader is able to decrypt the data *DN* from *En* (*K_N, DN*) and then verifies whether MAC is correct. If the recomputed MAC is consistent with the MAC received from the smart node, the reader considers the MAC is correct and the data set is authentic. Otherwise, the *En* (*K_ N, DN*) is changed by an adversary node. To avoid being detected for changing data, an adversary may launch old message replay attack by replacing a new message from a node with an old message from the node. When a reader forwards the *N* and *Nonce* to the central server, the central server can easily detect outdated nonce values which were reported previously. As a result, the old message replay attack can be detected. Once a smart node *N* is compromised, its individual Key *KN* is exposed and the adversary can derive all previous temporary keys to decrypt data in the old messages. Thus, it is important to achieve the backward security by updating the individual key periodically. However, periodically distributing new keys from a central server to all smart nodes incurs expensive communication cost. Therefore, the model uses a key hash chain method to avoid the key distribution cost.

In a large-scale system with a large amount of nodes, it could be an expensive and time-consuming operation to find the individual key of a specific smart node among all nodes' keys. The searching time is linear to the total number of nodes. The model consists of two methods to resolve this problem. First, method is to compute individual keys in run time rather than storing all keys in advance and searching keys on-demand. To this end, the central server maintains a secret key *Kc*. For each node with the tag ID *N*, its individual key *KN* is computed by the cryptographically secure hash function.*H* with *Kc*, i.e., $KN = H(N|Kc)$. In this way, the server does not need to store any individual keys. When receiving the tag ID *N*, the server directly recomputes $H(N|Kc)$ and obtains the

individual key *KN*, which avoids the searching. Since the computation time of the hash function is independent of the number of nodes, the time for finding individual keys can be significantly reduced in large-scale systems compared to linear searching.

DATA SELECTIVE FORWARDING

In the cluster-head based transmission algorithm, the cluster head in each cluster is responsible for forwarding the tag data of all cluster members to the reader. A malicious cluster head can drop part of the data and selectively forward the gathered information to the reader. Since an RFID reader may not know all the smart nodes in a head's cluster in advance, it cannot detect such attacks. To prevent the selective forwarding attack, it can exploit the cluster-member based data transmission algorithm, in which all cluster members hold the data of all other nodes in the cluster. A reader can compare cluster members' reported data with the cluster head's reported data to verify the correctness of the latter. The model use *Dall* to denote the set of all encrypted tag data (*N,Nonce,En*(*K_N,DN*),*MAC*(*K_N,N|DN*)) in a cluster .After node *N* collects encrypted data from all other nodes in its cluster, it creates its MAC on *DallN* and sends its (*N,Nounce,MAC*(*K_ N,N|DallN*)) to the reader. After receiving *Dallc* from a cluster head and the MACs of *Dall* from cluster members, the reader can verify the authenticity of *Dallc.* Based on a cluster member's *N* and *K_ N*, the reader creates *MAC* (*K_ N, N|Dallc)* and compares it with the received *MAC* (*K_ N, N|DallN*) from node *N*. If two MAC values are different, it means that the data from the cluster head or from node *N* is not valid. After conducting many comparisons for many cluster nodes, if the majority comparisons are valid, then the data from the cluster head should be valid, otherwise, it is not valid. Obviously, it causes excessive communication cost if the reader needs every cluster member to send its MAC for *Dall*. A simple solution is to let the reader only collect MACs from *T* (*T* 1) number of cluster members. Once *T* numbers of MACs are collected, the reader verifies the authenticity of the data set and considers it valid if all the MACs are correct. However, this method cannot prevent the collusion attack of multiple compromised nodes. Suppose that a node sent a pruned data set to the reader, other *T* compromised nodes can compute valid MACs for the pruned data set and send them to the reader. To prevent the collusion attack, it proposes a secure randomized solution, in which each smart node randomly decides whether to send its MAC to the reader. Suppose *F* is a cryptographically secure pseudo-random function which uniformly maps the input values into the range of [0*,* 1]. Each node *N* checks the inequality *F* (*N*|*K_N*) < *(*0 < < 1)*,* where *is* a threshold which decides the expected number of MACs the reader will receive. If the inequality holds, the node sends its MAC to the reader. Otherwise, it does not. As a result, each smart node in the cluster has a probability of ρ to send its MAC to the reader. When the reader receives the MAC from a smart node *N*, it recomputes *F* and accepts the MAC only when the inequality holds. Once the reader finds that all received MACs are correct, it considers the data set valid and complete. In this way, the collusion attack is prevented through verifying the legitimacy of nodes for providing their MACs, while the communication cost between the nodes and the reader is reduced. The threshold ρ is a system parameter loaded into the tag nodes and servers when the system is initialized. Larger threshold means stronger security strength at the expense of higher communication cost. The threshold ρ is initially decided by the users according to their security strength demand.

SOFTWARE ANALYSIS

The method has been implemented using the NS2 SIMULATOR tool, which is very easy to implement rather than implementing in hardware systems. Simulation quickly evaluate design alternative. It also evaluates complex functions for which closed form formula or numerical techniques not available.NS-2 is a discrete event driven simulation Physical activities are translated to events. Events are queued and processed in the order of their scheduled occurrences Time progresses as the events are processed.NS2 covers a very large number of applications, of protocols, of network types, of network elements and of traffic models. It is called as simulator objects. The goal of our notes is twofold: on one hand how to use an NS2 simulator, and on other hand to become acquainted with to understand the operations of some operations of some of simulated objects using NS2 simulations. Simulations may differ from each other in many aspects: the applications, topologies, parameters of network objects and protocols used. An alternative simple way to know about other possibilities for choosing network elements, network protocols or their properties is to directly at the library files that define them.NS2 is based on two languages: an object oriented simulator, written in C++ and an OTCL interpreter, used to execute user command scripts. NS has a rich library of network and protocol objects. There are two classes hierarchy: the compiled C++ hierarchy and the interpreted OTCL one, with one to one correspondence between them.

SIMULATION RESULTS

The performance between the RFID model and the Hybrid model can be explained using different parameters in order to improve the efficiency of the data. The parameters taken are Throughput, Packet delivery ratio. The figure 3 shows the transmission of data with the figure 4 shows the cluster head determination later the screen shots i.e. figures represent the parameters considered for Throughput, Packet delivery ratio.

Figure 3 Transmission of Data

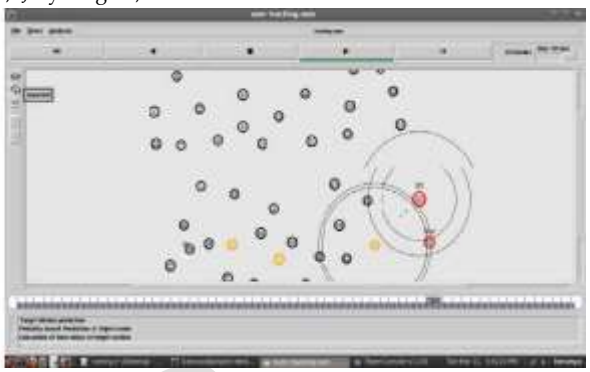


Figure 4 Cluster Head Determination

VARIATION OF THROUGHPUT BASED ON TIME

Throughput can be defined as the ratio of number of packets received to the time in seconds. The variation of throughput based on time is illustrated in the figure 5. The proposed hybrid model which increases the packets of 4023.2 which is more compare to RFID model which produces 3471.8 packets as shown in table 1. Thus the performance of proposed hybrid method has been proved to be efficient from the simulation result.

	THROUGHPUT	
TIME	RFID	HYBRID MODEL
0	0	0
10	2993	3634
25	3155	3854
50	3476	3944
75	3823	4122
100	3912	4562
AVERAGE	3471.8	4023.2

Table 1 Variation of Time with Throughput

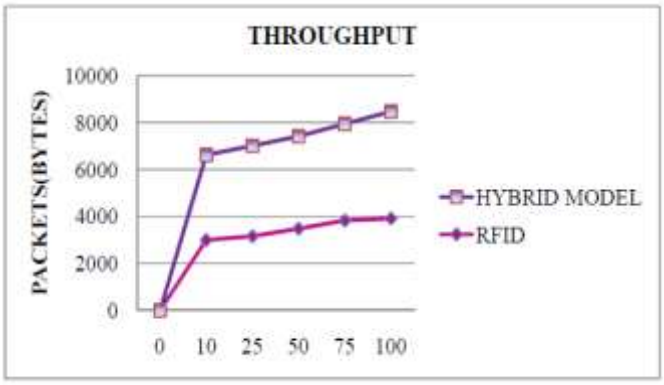


Figure 5 Variation of Time with Throughput

VARIATION OF PACKET DELIVERY RATIO BASED ON TIME

Packet delivery ratio (PDR) can be defined as the ratio of number of packets send to the packets received. The variation of packet delivery ratio based on time is shown in the figure 6. The proposed hybrid model which increases the PDR of 93.6% which is more compare to RFID model which produces 89.8% as shown in table 2, which increases the PDR up to 4.06 % in the Hybrid model. Thus the performance of proposed hybrid method has been proved to be efficient from the simulation result.

	PACKET DELIVERY RATIO	
TIME	RFID	HYBRID MODEL
0	0	0
10	87	91
25	89	93
50	90	94
75	91	95
100	92	95
AVERAGE	89.8	93.6

Table 2 Variation of Time with Packet Delivery Ratio

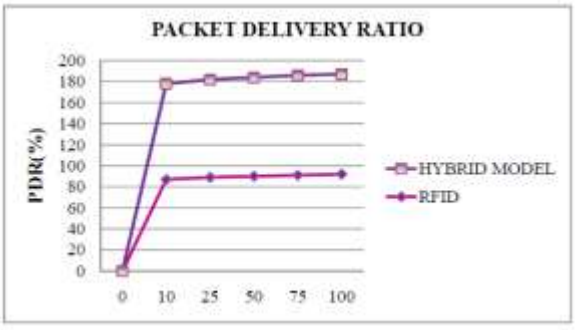
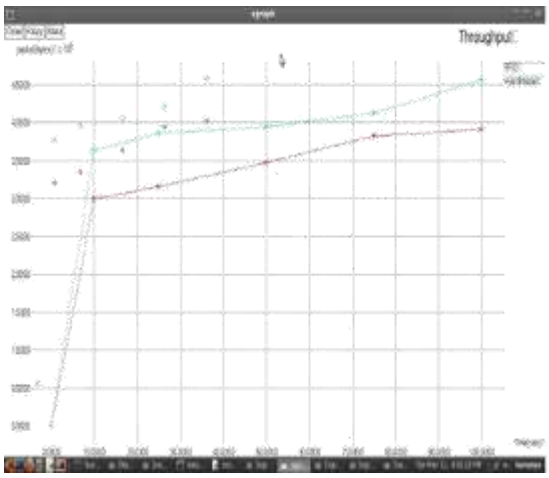


Figure 6 Variation of Time with Packet Delivery Ratio



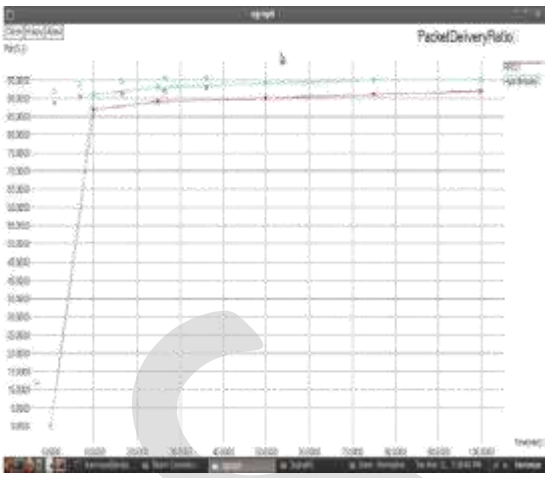


Figure 7 Throughput Figure

8 Packet Delivery Ratio

Figure 7 shows the Variation of time with throughput with the figure 8 of Variation of time with packet delivery ratio.

CONCLUSION

The concept has been implied Hybrid RFID and WSN system (HRW) that synergistically integrates the traditional RFID system and WSN system for efficient data collection. HRW has hybrid smart nodes that combine the function of RFID tags, the reduced function of RFID readers and wireless sensors. Therefore, data can be quickly transmitted to an RFID reader through the node that firstly reaches it. Instead of waiting for RFID readers to read data, smart nodes replicate packets with neighbor nodes using special reduced functional RFID readers. The collected packets are sent to a RFID reader when one of the replica nodes moves into the range of the RFID reader. Thus the proposed method enhances data transmission algorithms and security mechanisms to improve the data transmission efficiency, protects data privacy and avoids malicious data selective forwarding in data transmission. The simulation result improves the performance of HRW in terms of the cost of deployment, transmission delay capability, and tag capacity requirement.

REFERENCES:

[1] Chenxi Qiu, Haiying Shen (2013), "A Delaunay-based Coordinate-free Mechanism for Full Coverage in Wireless Sensor Networks", IEEE transaction on parallel and distributed systems, pp1-10.

[2] Chiara Petrioli, Michele Nati, Paolo Casari, Michele Zorzi, and Stefano Basagni (2013)," ALBA-R: Load-Balancing Geographic Routing Around Connectivity Holes in Wireless Sensor Networks" ,IEEE transaction on parallel and distributed system, Vol.,No.,pp1-9.

[3] Huang Lu, Jie Li, Sen, Mohsen Guizani (2012), " Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks" , IEEE transaction on parallel and distributed systems,pp.1-10

[4] Huan Zhou, Jiming Chen, Hongyang Zhao, Wei Gao and Peng Cheng (2013), " Exploiting Contact Patterns for Data Forwarding in Duty-cycle Opportunistic Mobile Networks" , IEEE transaction on mobile computing, Vol.9,No.3,pp317-332.

[5] Hui Lin and Halit Ü ster (2013), " Exact and Heuristic Algorithms for Data- Gathering Cluster-Based Wireless Sensor Network Design Problem" , IEEE transaction on networking,pp1-14.

[6] Ingook Jang, Suho Yang, Hyunsoo Yoon, and Dongwook Kim (2013)," EMBA: An Efficient Multihop Broadcast Protocol for Asynchronous Duty-Cycled Wireless Sensor Networks" ,IEEE transaction on wireless communications,Vol.12,No.4,pp1640-1650.

[7] Jian Li Yun Li Jian Ren Jie Wu(2013) " Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks" , IEEE transaction on parallel and distributed systems,pp.1-10

[8] Jiliang Wang, Yunhao Liu, Yuan He, Wei Dong, and Mo Li (2013), " QoF: Towards Comprehensive Path Quality Measurement

in Wireless Sensor Networks" , IEEE transaction on parallel and distributed systems,pp1-10.

[9] Jin Wang, Yue Yin, Jianwei Zhang, Sungyoung Lee and R. Simon Sherratt (2013), " Mobility based Energy Efficient and Multi-Sink Algorithms for Consumer Home Networks" ,IEEE transaction on consumer electronics,Vol.59,No.1,pp 77-84.

[10] Maria Gregori and Miquel Payaró (2013), " Energy-Efficient Transmission for Wireless Energy Harvesting Nodes" ,IEEE transaction on wireless communication,Vol.12,No.3,pp 1244 – 1254.

[11] Ruitao Xie, and Xiaohua Jia (2013), " Transmission Efficient Clustering Method for Wireless Sensor Networks using Compressive Sensing" ,IEEE transaction on parallel and distributed system,pp1-11.

[12] Rui Tan, Guoliang Xin, Jianping Wang and Hing Cheung (2010), " Exploiting Reactive Mobility for Collaborative Target Detection in Wireless Sensor Networks" ,IEEE transaction on mobile computingVol.,No.9,pp317-332.

[13] Yuan Song, Bing Wang, Zhijie Shi, Krishna Pattipati, Shalabh Gupta (2013), " Distributed Algorithms for Energy-efficient Even Self-deployment in Mobile Sensor Networks" ,IEEE transaction on mobile computing,pp1-14