Secure Data Transmission in Hybrid Radio Frequency Identification with Wireless Sensor Networks

P. S. Mano[1],
Dept. of Information Technology,
Kongunadu College of Engineering and Technology,
Trichy, India.

G. Karthik[2],
Dept. of Information Technology,
Kongunadu College of Engineering and Technology,
Trichy, India.

S. Kaarthiga[3],
Dept. of Information Technology,
Kongunadu College of Engineering and Technology,
Trichy, India.

G. Gowrishankar[4]
Dept. of Information Technology,
Kongunadu College of Engineering and Technology,
Trichy, India.

***Abstract*— Radio frequency identification (RFID) and wireless sensor networks (WSN) have been popular in industrial field. RFID and WSN are used to monitoring and senses the environmental conditions then send the data. In this article we propose RFID with WSN as Hybrid RFID and WSN (HRW). HRW that combines the RFID system and WSN device for efficient data collection. It is used to senses the signal from the environmental condition and stores the data in the database server. The user may collect the data from the back end server for data management. The database server uses the clustering to store the same data type in the same location. And it also reduces the time consumption while retrieval of the data. We also introduce the security mechanism in data transmission. It improves the performance while data transfer to other readers. This security mechanism protects the data and avoids the malicious attacks from the unauthorized user. High performance of HRW in terms of the cost of distribution, communication interruption and ability, and tag size requirement.**

Index Terms*— Radio frequency identification, wireless sensor networks, distributed hash table, data routing, clustering.

I. INTRODUCTION

Radio frequency identification (RFID) and Wireless sensor networks (WSN) has been very popular in the industrial field. They are used to observing the applications in the environmental surroundings. Wireless sensor network (WSN) is a group of specialized transducers with a communications infrastructure for observing and recording circumstances at diverse positions. Commonly observed parameters of the environmental situations are temperature, humidity, pressure, direction of wind and speed, brightness intensity, shaking intensity, noise intensity, power-line voltage. RFID is wireless technology radio waves that are used to transfer the data between RFID tags and RFID readers. RFID tags are used in many industries and also used to track the movement work in the atmosphere. The RFID readers are used to store the data in the local servers.

RFID tags are used to collects the data and which is directly communicates with the RFID readers. The communication of the readers with RFID tags are in the particular range of the periodical. If there are many tags are moved to reader at the same time, they will oppose to access the channels for information transmission. The positive transmissions of tags are in the percentage of 34.6 to 36.8 [1]. Such a transmission in RFID data collection is not a sufficient to meet the requirements of the low financial cost, high performance, and real time specific large-scale mobile monitoring applications. One of the drawbacks of RFID readers are not quickly transmits the data to the RFID tags. Due to the immobility and short range of the communication. Massive readers of RFID have to increase the coverage area and the communication transmission speed. This could cause the significant cost if the system deployment and design it considering the high cost and high quality of RFID readers. The high cost that occur between the RFID readers and the back-end servers. Thus the RFID readers can get the efficient data transmission.

In old-fashioned RFID observing applications such as in airline luggage system tracking technique the reader us required in quickly process several tags in the dissimilar distances. The reader communicates within the coverage session of the particular area. So these kinds of the problems can be avoided by using the multi-hop transmission. In the monitoring applications the objects can be monitoring by the variation of particular change in environment (e.g. body temperature, blood pressure) is the most important retrieval in objects. In this paper the proposing technique is the Radio frequency identification (RFID) and Wireless sensor networks (WSN) as Hybrid RFID with WSN (HRW). That integrates HRW to data transmission for energy efficient data collection in large scale monitoring for moving objects. HRW has new type of nodes they are called as Hybrid smart nodes. It combines the function of RFID tags and reduced the function of wireless sensor and RFID readers.

The HRW contains three types of components. They are smart nodes, RFID readers and backend server. The RFID reader collects the information [4][6][8][12] from the smart nodes and stores the details in the backend server. The data transmission that uses the multi hop transmission mode. Multi-hop transmission waits for data that received from the smart nodes to readers. The smart nodes are always in active manner. Then only it receives the data from the readers. If it is in deactivate mode it doesn’t receives the info. In traditional WSN a node in sleep mode it can’t receive and forward the data. In HRW a node can read the data from the tag even the nodes are in sleep modes, it increases the transmission speed. To improve the information collection it using the clustering concept. The cluster nodes is replicated their data to which data that belongs to. We also proposes the tag clean up algorithm, it removes the delivered data from the tags. It increases the size of the storage and reduces transmission overhead. While transmitting the data to one another smart node it having the security mechanism. It avoids the malicious attacks from the unauthorized users.

II. RELATED WORK

A. Hybrid Smart Nodes

Hybrid RFID and WSN (HRW) is used in the existing system. It has the smart nodes that integrate the RFID function and WSN function. The smart nodes are having the following components:

1) Reduced function sensor

In normal sensors they are having only transmission function but this sensor not only using for transmission it collects the atmosphere conditions and sensed data.

2) RFID tag

In RFID tags they are only serves the information to the storage buffer. The RFID tag receives the message and then responds with its identification and other information.

3) Reduced-function RFID reader (RFRR)

It is used for data transmission between the smart nodes. The smart nodes that are used to the RFID reader to read other nodes, tags and write their own information.

RFRR is used to help in the storing of sensed data and monitoring the environment. As comparison between RFID tags and HRW, HRW achieves higher performance in each node in RFRR. The nodes with joint RFID tag and sensor functions can also use HRW for efficient data collection with RFRR modules. Smart nodes are containing two state modes they are sleep and active mode. In active mode the sensor nodes can collects the information from the environment [4], [6]. And in sleep mode they do nothing.

B. Data Transmission Process

The Fig. 1 shows the architecture diagram of RFID and Fig. 2 mentions that architecture diagram of HRW system. RFID contains two layers upper and lower layers. Upper layer that was connected to the backend servers with high speed backbone cables. Lower layer is designed by a substantial number of article hosts that transfer data to RFID readers.

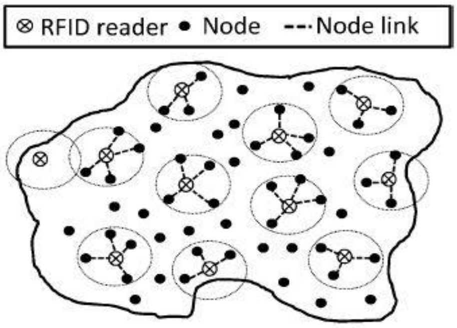

Fig. 1. Traditional RFID architecture

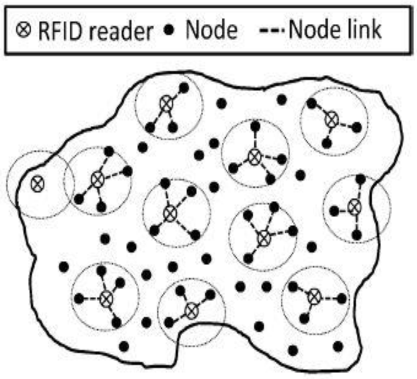

Fig. 2. HRW architecture.

In RFID architecture the nodes that are only in transmission range it communicates to RFID readers and it contain direct transmission. In HRW architecture, nodes are that can exchange and replicate node details with each other. This was the major difference between RFID and HRW architecture.The data transmissions in the RFID readers are in the multi-hop transmission mode. Each reader can receive the data information from the other outside readers of its particular range. HRW can collect the information and send to readers in high speed communication[8].

After smart node A gathers the identified data, it attaches the identified data with a timestamp and stores the data in its tag through RFRR. Its process contains four steps. In the step one process after the sensor unit in a smart node gathers the information about its tag host. In the second step it enquires RFRR to store the information into its tag. The third step includes once two nodes move into the transmission range of each other, the RFRR in a node delivers the information stored in another node's tag. Finally the step four is based on the host ID and timestamp, the node checks if tag has stored the information beforehand. If not, the RFRR then stores the attained information into the local tag.

The data of the node can be stored into the nodes in other system during exchange process. And the RFID reader can send the data to the reader. RFID reader can increase the number of readers to the delivery process.

When a node enters into the reading range of an RFID reader, the reader reads the information in the node's tag. The first entered node is assigned highest priority then later nodes.

TABLE I PSEUDO CODE OF THE PROCESS OF INFORMATION REPLICATION EXECUTED BY SMART NODE I.

```
if this.state =active then
Collect the sensed info of its host Hi
Store (Hi, tagi)
for every node j in its transmission range do
if this.linkAvailable (j) then
Read info Hj with timestamp > tij from tagj
Store (Hj, tagi)
Update timestamp tij with current time
end if
end for
end if
```

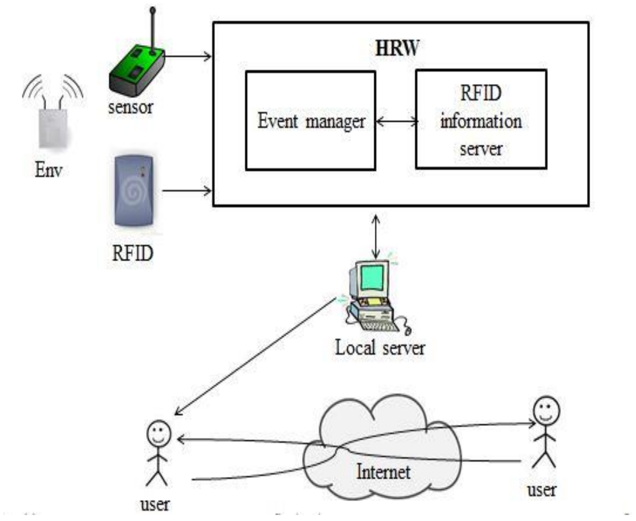

Fig. 3. System architecture of HRW

III. System Architecture

Figure 3 that clearly explain about the Hybrid RFID and WSN system. It integrates function of the Radio frequency identification and Wireless sensor networks. The description of the architecture is, it senses the environmental circumstance in the specific area. But it doesn't act in the particular specified area monitoring. It senses signal if any variation the held in the occasion monitoring. The process of the RFID in the architecture is to tracing the particular occasion. The RFID consists of two components they are tags and readers. The tags are attached with all objects to identify the RFID system. The readers can communicate with the tags through the RF channel to obtain the information. Reader contains the records. It stores the information of data in the databases. The databases having replicated information, if the data that loses in the databases we can get the data from the readers. Wireless sensor network is used to monitor the physical environmental condition changes in the particular area. The both RFID and WSN integrate as the Hybrid RFID and WSN (HRW). The function HRW contains two components they are event manager and RFID information server. The communication between the event manager and the RFID information server is a bi-directional. The event managers' process is to collects the information and stores the details. It events are held in the environment changes. The RFID information server that stores the information in the backend server.

The collected information that stored in the server. And the received information that passes to the local server. The process of the local server stores the data in database. The storage of the data in same location. It reduces the time consumption for searching of the data. This method is called as clustered based transmission. Clusters can then easily be defined as objects belonging most likely to the same distribution. In the HRW system, since the data is stored in tags, active nodes can recover the information at any time from a sleeping node.

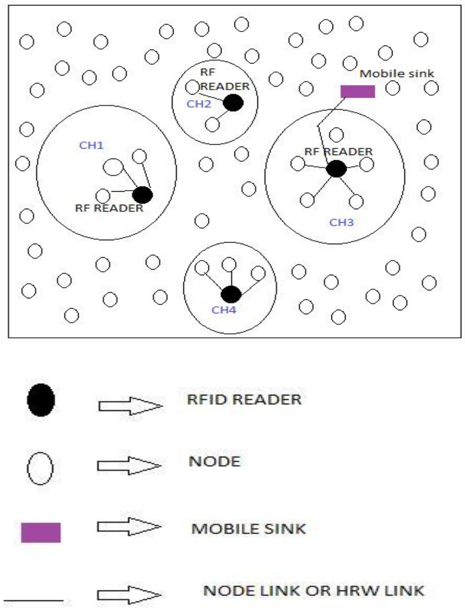

Fig. 4. Data transmission from one to another node using RFID reader.

Data transmission from one to another node using RFID reader. In old-fashioned WSNs, moreover, nodes in deactivate mode cannot conduct data transmission. Therefore, the HRW system can greatly improve packet transmission efficiency with the RFID technology.

The database is used to store the data in the local server. If the user wants to send the data from one user to another user the internet communication is using. Here no secure process while sending data from one user to another user.

This RFID reader reads the data from the coverage area. It senses the signal from the environment and transmit the data to the local server of the user. Here tag cleanup algorithm also used for clear memory in the senders delivered data. This increases the memory of the databases. We can store large data types in the memory allocated for the particular data.

IV. SECURITY MECHANISM

The multi-hop data transmission method in HRW improves the communication efficiency. The attacker may easily access the data while sending data one node to another. The attacker can obtain all the information in the compromised nodes and use the compromised nodes to obtain sensitive information and disrupt system functions. This process needs the security policy while transferring data to another node. It adds the authentication and authorization to the user when the users access the data. It gives the secured access in the data to authorized user. So in this section, we consider two security threats arising from node compromise attacks: data manipulation and data selective forwarding[10].

A. Data Privacy And Data Manipulation

The process of data privacy and data manipulation, each smart node replicates its information to other nodes. Once a node is cooperated, all the information of other nodes is visible to the challengers, which is dangerous especially in privacy sensitive applications such as health monitoring.

A mischievous node can also use the gathered information and provide wrong information to the readers. Moreover, it is important to safeguard the confidentiality and authenticity of tag information in data transmission. The challenge in the process of data privacy is to share the data, while protecting personal information. The process of the data manipulation is to take the data and manage into the easiest method of reading. The protection of the tag information in data transmission needs the security process. It needs public key encryption or private key encryption technique. This method use to collect or dissemination the data in secrete manner. Public key actions are too exclusive for the smart nodes due to their partial computing, storage and bandwidth resources. We then improve a symmetric key based security scheme in our system. In this novel, we concentration on the threats due to the compromised smart nodes and assume the readers are secure. In our security system, the process uses the Kerberos algorithm. Kerberos technique is a networks authentication protocol which works on the basis of ticket granting system. It allows nodes which contains the tickets. In the process of the Kerberos is an authenticated server, which forwards the user name to key distributing server. This process never sends the secret key to the user unless it is encrypted by user. The Kerberos authentication process having more benefits. Such as more secure, flexible and efficient. The key distributing server issues the ticket to the client. It includes the timestamp value. The timestamp values access its value in the particular session. If the value of the session is ends then the ticket value is not valid. Kerberos process uses the private key encryption. The process encode and decode it uses the same key value. Kerberos algorithm builds on symmetric key value of authentication and requires a trusted third party.

User client login process includes two steps. In the first step user enters his name and password in the server. The next step client transforms the password into the symmetric key distribution. Client authentication process, this process includes three steps. In step one the client sends message of the user ID to the authenticated server (AS).

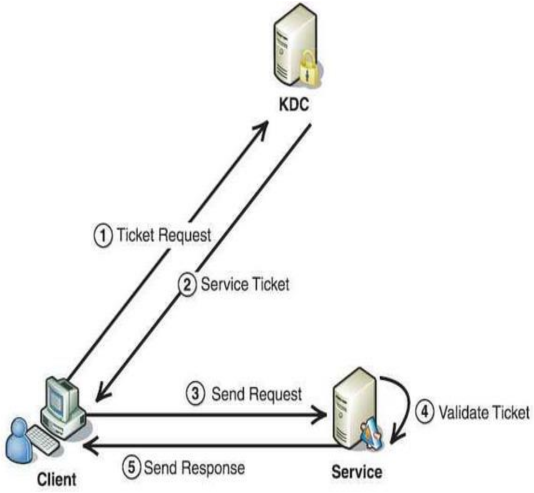

Fig. 5. Kerberos process

The AS creates the secret key. Second step AS checks whether the client in its databases or not. If the client in its database AS sends back the following messages. Ticket granting service (TGS) key encrypted using secret key of the client and the valid period of the ticket that issues by AS. In third step, when the user receives the messages, they can decrypt data, if the key that not matches in DB user can't access the data. Client service authorization, this process that client sends the messages to TGS. Next the received message of TGS, it retrieves message of TGS secret key. Client service request, the receiving messages from TGS, the client has access the data. We propose distributed key storing in the back-end servers to store the usable key from the AS. We form the back-end servers into a distributed hash table (DHT). The DHT overlap supplies Insert (key, data) and Lookup (key) functions [7]. The ticket giving process in this novel proposed the advantage in accessing the known user to get the data. It allows the user who having the ticket while accessing the data. The process that mention user want to get the ticket from the trusted third party.

B. *Data Selective Forwarding*

This process includes the clustering concept. The clustering is the task of grouping set of data's in the same group. Or it has the data in similar data type. Its main task is to store the data in the memory location. In the cluster-head based broadcast algorithm, the cluster head in all nodes in cluster is responsible for forwarding the tag data of all cluster members to the reader. A mischievous cluster head can drop part of the data and selectively accelerative the collected information to the reader. Subsequently an RFID reader may not know all the smart nodes in a head's cluster in advance, it cannot identify such attacks. To avoid the selective forwarding attack, we can implement the cluster-member based data transmission algorithm, in which all cluster members clutch the data of each other nodes are in the collection. The process of data selective forwarding, select the particular node and send the data. It reduces the transmission cost, because the data sends to the node only requests by that original node. It increases the data transmission process in high speed to reach another user.

V. PERFORMANCE AND EVALUATION

Fig 6 shows the transmission links between hosts are usually alternatingly connected, we created a delay tolerant network environment for the performance evaluation. The situation where there is no movement arrangement and use the real traces to simulate the condition where there is movement arrangement for the applications where monitored substances (e.g., birds, animals, people) tend to move in clusters. In the epidemic transmission, the packets of nodes are replicated to other nodes within TTL hops, which was set to 6 by default. In the source replication transmission, a source node allows a certain number (10 by default) of nodes to read its packets. We matched these methods with the ‘‘direct’’ communication method in the old-fashioned RFID systems, in which a node keeps its collected information in its tag until it reaches the kind of an RFID reader.

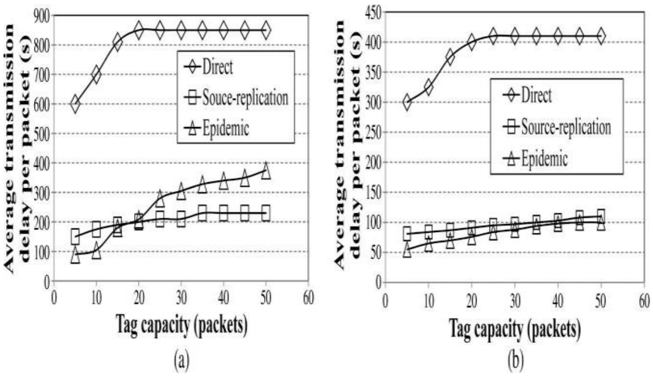

Fig. 6. Transmission delay versus tag capacity.

Larger reading range makes it easier for a node to find other neighbor nodes, which may either be the RFID readers or promising relay nodes moving to RFID readers. Epidemic and source-replication proactively transmit data to RFID readers using multi-hop routing, while the direct transmission lets nodes wait until meeting readers to transmit data. The result indicates the higher efficiency of the HRW transmission mode than the traditional RFID system.

Fig. 7 shows the comparison results of the average transmission delay versus the network size excluding readers when R ¼ 20 m and R ¼ 40 m, respectively. That the network size increases, the packet transmission delay of both algorithms decreases slightly. The reason is that given the same number of packets, increasing the number of nodes in the same area increases the node density. cluster-head has longer delay than source-replication. In the cluster-head method, the cluster head holds the replicas of the packets in the cluster and sends the replicas to an RFID reader when it meets an RFID reader. In the source-replication method, every node in a cluster holds a copy of packets from other nodes in the cluster. All information can be transmitted to an RFID reader whenever one cluster member meets an RFID reader, which greatly reduces the packet transmission delay. Source-replication has very slightly less number of delivered packets than other methods. As source-replication does not use the clean-up algorithm and the probability for a cluster member to meet an RFID reader is smaller with a small reading range, packets are more likely to be dropped because of the congestion.

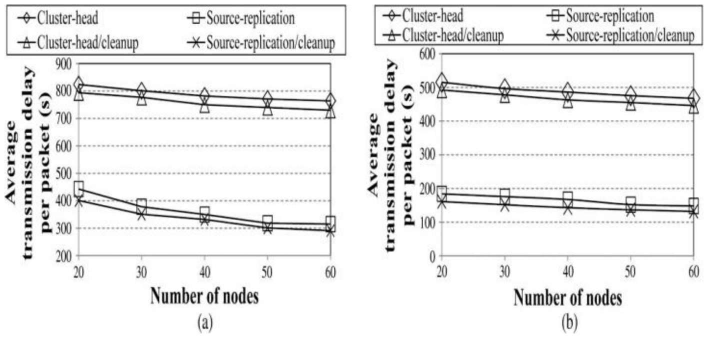

Fig. 7. Comparison of transmission delay versus network size

VI. CONCLUSION

This paper introduces the Hybrid RFID with WSN (HRW) that combines the multi-hop transmission and the direct data transmission mode in the RFID. HRW also improves the data collection in the process of RFID readers within the particular range of communication. HRW is composed of RFID readers and smart nodes. The RFID readers store the data in the backend servers. The user can retrieve the data at any time. The stored data were in the clustering analysis, which contains the same kind of data stored in the same type location. It reduces the time consumption, while retrieving the data and send to another client. In this novel we introduce the security mechanism Kerberos algorithm used to prevent the data. This secure method has ticket granting to user. It avoids malicious attacks from unauthorized users. The future work is to implement this paper in real world, that counting the number of wild animals in the forest and send the information to the authorized user to access the data from server.

REFERENCES

[1] B.H. Bloom, ‘‘Space/Time Trade-Offs in Hash Coding with Allowable Errors,’’ *Commun. ACM*, vol. 13, no. 7, pp. 422-426, July 1970.

[2] R. Clauberg, ‘‘RFID and Sensor Networks,’’ in Proc. *RFID Workshop*, St. Gallen, Switzerland, Sept. 2004.

[3] J.Y. Daniel, J.H. Holleman, R. Prasad, J.R. Smith, and B.P. Otis, ‘‘NeuralWISP: A Wirelessly Powered Neural Interface with 1-m Range,’’ *IEEE Trans. Biomed. Circuits Syst*., vol. 3, no. 6,pp. 379-387, Dec. 2009.

[4] D. Karger, E. Lehman, T. Leighton, M. Levine, D. Lewin, and R. Panigrahy, ‘‘Consistent Hashing and Random Trees: Distributed Caching Protocols for Relieving Hot Spots on the World Wide Web,’’ in Proc. STOC, 1997, pp. 654-663.

[5] C. Lee and C. Chung, ‘‘RFID Data Processing in Supply Chain Management Using a Path Encoding Scheme,’’ *IEEE Trans. Knowl. Data Eng.*, vol. 23, no. 5, pp. 742-758, May 2011.

[6] T. Lez and D. Kim, ‘‘Wireless Sensor Networks and RFID Integration for Context Aware Services,’’ *Auto-ID Labs, Cambridge, MA, USA*, Tech. Rep., 2007.

[7] M. Li, Y. Liu, J. Wang, and Z. Yang, ‘‘Sensor Network Navigation Without Locations,’’ in Proc. *IEEE INFOCOM*, 2009, pp. 2419-2427.

[8] H. Liu, M. Bolic, A. Nayak, and I. Stojmenovic, ‘‘Taxonomy and Challenges of the Integration of RFID and Wireless Sensor Networks,’’ *IEEE Trans. Netw*., vol. 22, no. 6, pp. 26-35, Nov./Dec. 2008.

[9] W. Luo, S. Chen, T. Li, and S. Chen, ‘‘Efficient Missing Tag Detection in RFID Systems,’’ in Proc. *IEEE INFOCOM*, 2011, pp. 356-360.

[10] K. Ren, W. Lou, and Y. Zhang, ‘‘LEDS: Providing Location-Aware End-To-End Data Security inWireless Sensor Networks,’’in Proc. *IEEE INFOCOM*, Apr. 2006, pp. 1-12.

[11] D. Simplot-Ryl, I. Stojmenovic, A. Micic, and A. Nayak, ‘‘A Hybrid Randomized Protocol for RFID Tag Identification,’’ Sensor Rev., vol. 26, no. 2, pp. 147-154, 2006.

[12] L. Zhang and Z. Wang, ‘‘Integration of RFID into Wireless Sensor Networks: Architectures, Opportunities and Challenging Problems,’’ in Proc. *Grid Cooperative Computing Workshop*, vol. 32, pp. 433-469, 2006.