An Integrated Adapted Key Management and Quality Data Delivery over Wireless Network

P. Raju
Ph.D Research Scholar,
Department of computer science,
Research and Development Centre,
Bharathiar University and Assistant Professor,
Cherran Arts and Science College,
Kangayem, Tiruppur,
Tamilnadu, India.

C. Chandra Sekar, PhD
Associate Professor
Department of computer science,
Periyar University,
Salem, Tamilnadu, India.

ABSTRACT

Wireless network broadcast the information with active node variance. Data delivery over wireless network is one of the key issues to be addressed. Many efficient data delivery methods are widely used in different network environments as they reduce the overhead traffic and delay. Hence they improve the network lifetime. However, they lack effective data delivery on different network environment and security. In this paper, to perform effective data delivery on different network environments, Routing Function Independent Data Delivery (RFIDD) scheme is introduced. The RFIDD scheme develops Observant Reasoning algorithms to identify concession nodes (i.e.,) packet dropping nodes. The Observant Reasoning (OR) algorithm provides suitable solution to ensure data delivery with average running formula in wireless network. OR-algorithm finds an optimal result in the sense that it recognizes every packet dropping nodes without introducing false negative rate. RFIDD Scheme also combines the Adapted Key Management Routing (AKMR) protocol to improve the security level while performing data delivery on wireless network. AKMR performs the encryption, authentication and decryption processes to attain higher security ratio in RFIDD Scheme. The integration of data delivery scheme with security measure is performed with three orders of magnitude which dynamically adjusts security level depending on the network state. In this paper, RFIDD scheme is analyzed to assess the data delivery ratio and packet dropping probability rate and compared to the state-of-the-art methods. RFIDD was also implemented NS2 and compared against Distributed Cache Invalidation Method and Redundancy Management of Multipath Routing to assess its performance experimentally. The security and average response time are reported versus several variables, where RFIDD showed to be superior when compared to the other methods.

Keywords

Function Independent, Data Delivery, Observant Reasoning, Concession nodes, Key Management.

1. INTRODUCTION

Caching data items in wireless network has received great attention with the increase in the wireless devices. Consequently there exist different methods addressed by several research persons in the area of data delivery over wireless networks. Distributed Cache Invalidation Method (DCIM) [1] performed update rates at the data source but at the cost of running average to estimate the inter update interval. On the other hand, Redundancy Management of Multipath Routing (RMMR) [2] addressed average formula using probability model. However RMMR failed to address effective data delivery and security. Voting-based Distributed Intrusion Detection (VDID) [3] algorithm was designed with the objective of providing security during data forwarding. Another Position-based Opportunistic Routing (POR) [4] was designed with the purview of providing reliable data delivery. Though data delivery and security was concentrated, the key issue, the packet dropping rate was not focused. The RFIDD scheme on the other hand, reduces the packet dropping rate by applying observant reasoning algorithm.

The success of 3rd generation wireless cellular networks provides significance with respect to data rate, delay and error rate. Offline and Online Optimization (OOO) [5] algorithm was designed to provide single user throughput. Dynamic enroute filtering [6] scheme was designed with the objective of improving the throughput in highly dynamic wireless networks. An accurate stochastic steady state throughput was designed in [7] aiming at not only improving the throughput but also to reduce the significant error during data forwarding. Another data dissemination method was introduced in [8] using Dijkstra’s algorithm. However, the average response time remained unaddressed in the above said methods. The RFIDD scheme on the other hand reduces the average response time by applying Adapted Key Management protocol.

Improving data delivery in Delay Tolerant Networks has received higher attention due to the short radio transmission range. In [9], Cluster-based routing protocol was introduced to achieve higher delivery ratio with lower overhead. In [10], Correlation Aware QOS Routing algorithm was designed for efficient delivery of visual information in wireless video sensor networks. Though efficient data delivery was addressed in the above methods, security remained unsolved. In [11] with the objective of providing security, a novel combination of group signature and ID-based encryption model was introduced for route discovery. Another problem faced in many wireless networks is the optimized relaying. In [12], Geographic Transmission with Optimized Relaying was introduced for addressing issues related to transmission.

Energy conservation and data delivery is the most significant part in wireless sensor networks (WSNs). Decentralized Fuzzy Clustering Protocol (DCFP) [13] was designed with the objective of improving the network lifetime through efficient data delivery. A novel Link Correlation-aware Opportunistic Routing (LCOR) [14] scheme was introduced to improve the rate of throughput. On the other hand, a probabilistic approach [15] was designed to improve the rate of throughput by reducing the total traffic load using handoff procedure. An analysis of throughput using cooperative communication was provided in [16].

The importance of wireless networks with increased number of sensor nodes cannot be overestimated. In [17], an anchor-based public key caching was introduced to reduce the average response time during source destination packet forwarding. However, packet dropping rate remained unaddressed. In [18], packet dropping rate was reduced significantly based on the fault tolerance mechanism. In [19], routing algorithm based on greedy method was designed with the objective of improving the packet delivery ratio. Another method to improve the bandwidth using traffic-aware data scheduling algorithm was introduced in [20].

By integrating these data delivery schemes with the security measure, a dynamic security model depending on the network state is ensured in wireless networks.

In the rest of this paper, Section 2 elaborates the contributions of the proposed scheme, Routing Function Independent Data Delivery. Section 3 provides an analytical analysis of the system, whereas Section 4 presents the discussion of proposed and existing methods with respect to different parameters. In this paper, a Routing Function Independent Data Delivery (RFIDD) scheme is proposed to perform effective data delivery on different network environments. First, based on the Observant Reasoning algorithm, a data delivery with average running formula is proposed to improve the data delivery ratio reduce the packet dropping probability rate by correlated sensors. Then, an Adapted Key Management Routing protocol is designed to improve the security.

Experimental results are discussed to measure the significance of proposed Routing Function Independent Data Delivery (RFIDD) scheme. Section 5 finishes the paper with concluding remarks.

2. PROPOSED ROUTING FUNCTION INDEPENDENT DATA DELIVERY (RFIDD) SCHEME

The RFIDD scheme has been designed to perform effective data delivery on different network environments that support a bidirectional communication between pairs of nodes. The block diagram of Routing Function Independent Data Delivery (RFIDD) scheme is shown in figure 1.

As shown in figure, the goal of RFIDD scheme is to identify the concession nodes (i.e. packet dropping nodes) to provide data delivery with average running formula. The second design goal of proposed scheme is to apply Adapted Key Management Routing protocol to perform encryption, authentication and decryption techniques while performing data delivery on wireless network aiming at improving the security. The elaborate description of the design of RFIDD scheme is provided in the following subsection.

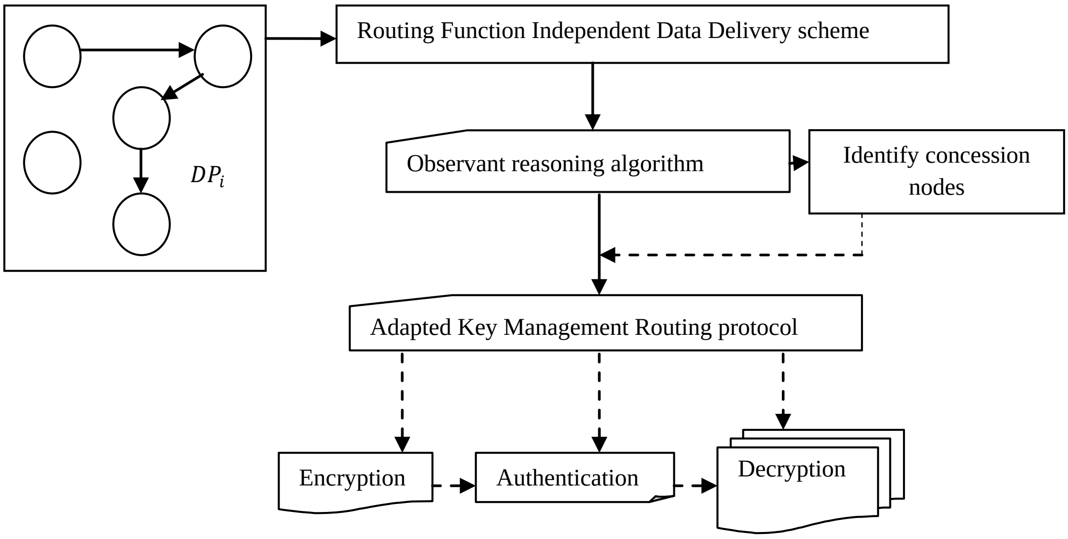
DP_i
Routing Function Independent Data Delivery scheme
Observant reasoning algorithm
Identify concession nodes
Adapted Key Management Routing protocol
Encryption
Authentication
Decryption

Figure 1 Block diagram of Routing Function Independent Data Delivery scheme

2.1 Observant Reasoning Algorithms

The first step in the design of the RFIDD scheme is to develop an Observant Reasoning algorithm. The RFIDD scheme develop Observant Reasoning algorithms to identify concession nodes (i.e.,) packet dropping nodes. Figure 2 shows the structure of packet dropping.

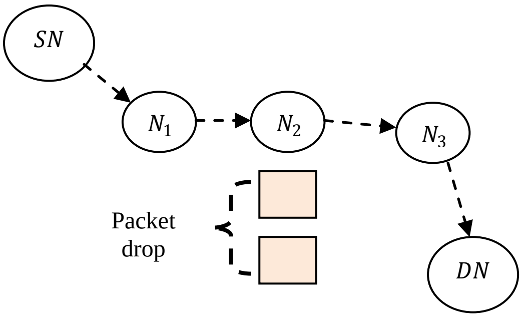

Figure 2 Structure of Packet Dropping

As shown in the figure, let us consider a source node ‘SN’, and a destination node ‘DN’ with three intermediate nodes ‘N_1’, ‘N_2’ and ‘N_3’ respectively. Here the source node sends the data packets continuously to the destination nodes through the intermediate nodes.

Let us further assume that the source node is aware of the route path through which the data packets has to be flow. The intermediate node ‘N_1’ sends the packet to ‘N_2’ whereas packet dropping is said to occur at the intermediate node ‘N_2’. In order to avoid packet dropping the Observant Reasoning (OR) algorithm in RFIDD scheme provides suitable solution to ensure data delivery with average running formula in wireless network. By applying OR algorithm, packet dropping nodes are identified.

In order to construct OR algorithm, a directed graph ‘$G = (V, E)$’ is designed. Here ‘G’ symbolizes the directed graph, ‘V’ represents the set of vertices that denotes the sensor nodes ‘$N_1, N_2, \ldots, N_n$’ whereas ‘E’ symbolizes the set of edges within the radius ‘R’ and is formulated as given below.

$$G = (V, E), Where\ V = \ N_1, N_2, \ldots., N_n \qquad (1)$$

An edge ‘$N_1, N_2\ \in E$’ if and only if ‘N_1’ is the neighbor of ‘N_2’ and vice versa. The packet dropping nodes in the network using observant model is formulated as given below.

$$PD = (t, N_1, N_2) \qquad (2)$$

From (2), the packet dropping is symbolized by ‘PD’, indicating that the sensor node ‘N_1’ observes an abnormal activity (i.e. packet drop) of sensor node ‘N_2’ at time ‘t’. Therefore, the packet information during each transmission includes the following, the source node ‘SN’, the destination node ‘DN’, number of data packets ‘DP_n’ and route path ‘$Route_p$’. The structure of packet information is provided in figure.

Source ode ‘SN’	Destination node ‘DN’	Route path ‘$Route_p$’	Number of data packets ‘DP_n’

Figure 3 Structure of packet information

From the above figure, the number of data packets defined plays a key role in identifying the packet dropping nodes. If all sensor nodes in wireless network are concession, then the base station cannot identify which sensor nodes are concession based on observant reasoning. Therefore, OR algorithm in RFIDD scheme introduced a threshold ‘δ’ so that the concession sensor nodes does not exceed the threshold ‘δ’. Figure 4 shows the Observant Reasoning algorithm.

```
Input: sensor nodes ‘$N_i = N_1, N_2, \ldots, N_n$’,
directed graph ‘$G = (V, E)$’, threshold ‘$\delta$’,
Number of data packets ‘$DP_n$’
Output: Reduced packet drop with improved packet
 delivery rate
Step 1: Begin
Step 2:   For each sensor nodes ‘$N_i$’ in directed graph ‘$G$’
Step 3:     Let $Neigh_i$ be the number of neighbors of ‘$N_i$’
Step 4:       If ‘$DP_n$’ > ‘$\delta$’
Step 5:       Occurrence of concession nodes
Step 6:         Measure packet dropping nodes using (2)
Step 7:         End if
Step 8:         If ‘$DP_n$’ < ‘$\delta$’
Step 9:           Normal flow of data packets
Step 10:        End if
Step 11:  End for
Step 12: End
```

Figure 4 Observant Reasoning algorithm

As shown in the figure, the OR-algorithm identifies the concession nodes in wireless network. With the objective of reducing the packet drop rate and ultimately improving the packet delivery ratio, to start with, a threshold for concession nodes is derived. Then, for each sensor nodes in the directed graph, the number of data packets is checked with the threshold to measure the number of concession nodes. Followed by this, the concession nodes are identified by average running formula through neighbor nodes. As a result, OR-algorithm finds an optimal result in the sense that it recognizes every packet dropping nodes without introducing false negative rate.

2.2. Adapted Key Management Routing (AKMR) protocol

The second step in the design of the RFIDD scheme is the construction of Adapted Key Management Routing protocol. The RFIDD scheme combines the Adapted Key Management Routing (AKMR) protocol to improve the security level while performing data delivery on wireless network. AKMR performs the encryption, authentication and decryption processes to attain higher security ratio in RFIDD Scheme.

In order to perform encryption, a Pair Key (PK) is established between the neighbor sensor nodes. Next, authentication is performed with the aid of Transmission Key (TK) to secure the data packets sent by a sensor node to its neighboring nodes.

Finally, Sensor Node Base Key (SNBK) is established to perform secure communication between the sensor node and the base station. As a result, only with the help of SNB key, decryption is performed.

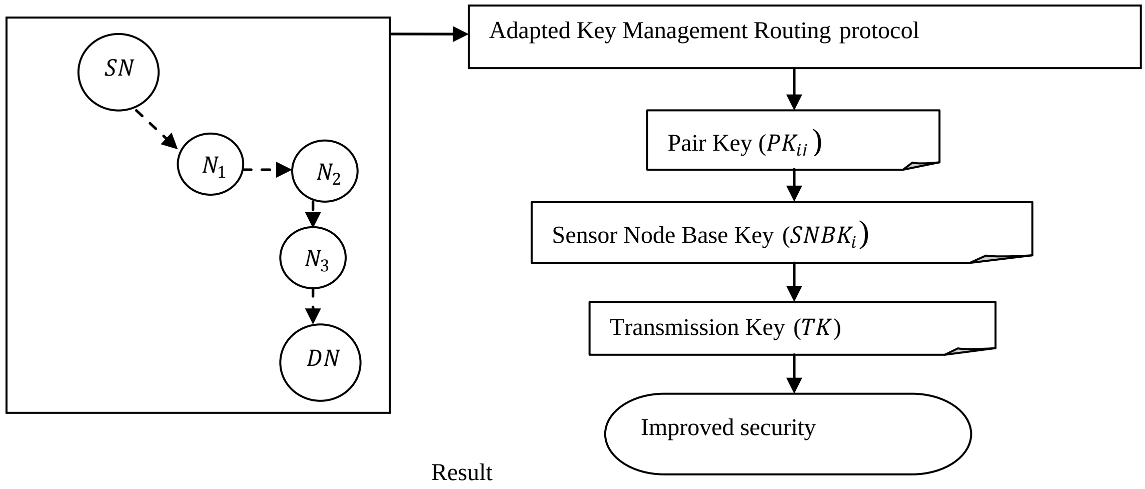

Figure 5 Block diagram of Adapted Key Management Routing protocol

Therefore, two phases are involved in the design of AKMR protocol, neighbor discovery phase and secure communication phase. Figure 5 shows the block diagram of Adapted Key Management Routing protocol.

As shown in the figure, during the neighbor discovery phase, the source (i.e. sensor) node broadcasts an ID to the sensor nodes that lie within the radius 'R'. Every sensor node (i.e. intermediate node) receiving the ID responds to it by sending an ID. In this way the source node identifies the neighboring senor nodes within the radius 'R' and neighbor discovery phase gets accomplished.

Once the neighbor discovery phase is completed, the Sensor Node Base (SNB) key and Pair Key (PK) are identified. The SNBK, PK and TK are mathematically formulated as given below.

$$SNBK_i = f(SN||i\ ||BS\ ||DN\ ||MK) \quad (3)$$

$$PK_{ij} = f(\mathrm{SN}||\min(i,j)||\max(j,i)||\ DN||\ MK) \quad (4)$$

$$TK = f(SN\ ||i\ ||DN||MK) \quad (5)$$

From (3), (4) and (5), '$||$' symbolizes the concatenation function, 'f' symbolizes the function to obtain the sensor node base key 'SNB_i'with a base station 'BS'. 'MK' is the master key that is distributed to all the sensor nodes in wireless network. The neighbor sensor nodes (i.e. intermediate nodes) are established based on the min max function. Finally, the transmission key is generated to secure the data packets sent by a node 'SN' to the destined node 'DN' respectively. Figure 6 shows the Key Management Routing algorithm.

```
Input: sensor nodes '$N_i = N_1, N_2, \dots, N_n$',
directed graph '$G = (V, E)$', threshold '$\delta$',
Number of data packets '$DP_n$',
Master Key '$MK$',Source Node '$SN$',
 Destination Node '$DN$', Base Station '$BS$'
Output: Improved security with minimum response
ne
Step 1: Begin
Step 2:  For each sensor nodes '$N_i$' in directed graph
,
Step 3:    Obtain the Master Key '$MK$'
Step 4:    Evaluate Sensor Node Base Key using (3)
Step 5:    Evaluate Pair Key using (4)
Step 6:    Evaluate Transmission Key using (5)
Step 7:    End for
Step 8: End
```

Figure 6 Key Management Routing algorithm

As shown in the figure, to improve the security during data delivery on wireless network, the Key Management Routing algorithm is designed. The Key Management Routing algorithm performs encryption, authentication and decryption to attain higher rate of security in RFIDD scheme. Finally, the integration of data delivery scheme with security measure with three orders of magnitude (i.e. Sensor Node Base Key, Pair Key and Transmission Key) dynamically adjusts security level depending on the network state.

3. EXPERIMENTAL SETTINGS

In this section, the numerical data obtained as a result of applying RFIDD scheme is presented. Table 1 lists the set of input parameter and evaluates performance of RFIDD scheme via simulation. For example WSN consists of 70 sensor nodes deployed in a square area of A^2 (1200 m * 1200 m) placed in a random manner in the wireless sensor network that generates traffic for every 10 m/s.

The nodes are distributed in an area using Random Way point model for simulation, whereas the link layer provides the link between two sensor nodes and the design of link is multi direction. The radio ranges are dynamically adjusted between 5m and 30m to maintain network connectivity. The base station collects the data packets of range 9 – 63 and forwards the data packets to the base station with each data packet size differing from 100 KB to 512 KB. The simulation time varies from 500 simulation seconds to 1500 simulation seconds.

Table 1 Simulation Parameters

Parameters	Values
Network area	1200 m * 1200 m
Number of nodes	10,20,30,40,50,60,70
Number of data packets i.e., number of data block	9, 18, 27, 36, 45, 54, 63
Size of data block (i.e., packet)	100 – 512 KB
Range of communication	30m
Speed of node	0 – 10 m/s
Simulation time	1500 s
Number of runs	7

4. DISCUSSION

In this section, the result analysis of RFIDD scheme is made and compared with two existing methods, such as Distributed Cache Invalidation Method (DCIM) [1] and Redundancy Management of Multipath Routing (RMMR) [2] in WSN. To evaluate the efficiency of RFIDD scheme, the following metrics like data delivery ratio, packet dropping probability rate, data delivery security, average response time in Wireless Sensor Network is measured.

4.1 Impact of data delivery ratio

Data delivery ratio is the ratio of successfully received data packets by the base station to the total packets being sent from the source sensor nodes. The mathematical formulation of data delivery ratio is as given below.

$$DDR = \frac{DP_r}{DP_s} * 100 \qquad (6)$$

From (6), the data delivery ratio 'DDR' is measured using the data packets received 'DP_r' to the data packets sent 'DP_s'. It is measured in terms of percentage (%). Higher the data delivery ratio, more efficient the method is said to be. The values obtained through (6) is tabulated for different data packets using the proposed RFIDD scheme and compared elaborately with the existing two works namely DCIM [1] and RMMP [2] respectively.

Table 2 Tabulation for data delivery ratio

Data packets (KB)	Data delivery ratio (%)		
	RFIDD	DCIM	RMMP
9	74.39	64.19	53.17
18	78.73	66.70	55.65
27	80.23	68.20	59.15
36	75.31	63.28	54.23
45	78.16	66.13	57.08
54	81.32	69.29	60.24
63	84.98	72.95	63.90

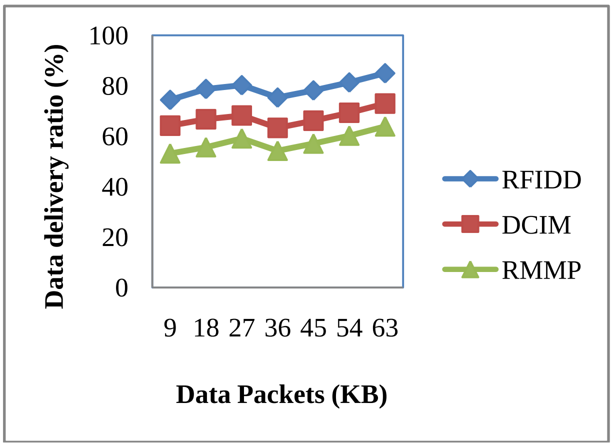

Figure 7 Measure of data delivery ratio

Figure 7 depicts data delivery ratio of three methods RFIDD, DCIM [1] and RMMP [2]. It is found that the data delivery ratio using RFIDD scheme is increases as the data packets increases, though not found to be linear. When the data packets are high, more nodes are available for data forwarding and this increase the data delivery ratio. On the other hand, the non-linearity observed in the graph is because of the different data packets are sent through various sensor nodes and each sensor nodes has its own data delivery rate. The proposed RFIDD scheme has maintained constant data delivery ratio throughout the simulation scenarios because it uses Observant Reasoning algorithm to identify concession nodes (i.e.,) packet dropping nodes. As a result, the concession nodes are identified by average running formula through neighbor nodes that results in the improvement in data delivery ratio using RFIDD scheme by 14.90% compared to DCIM and 27.11% compared to RMMP.

4.2 Impact of packet dropping probability rate

Packet dropping probability rate is the ratio of number of packets dropped by the intermediate sensor nodes to the total packets being sent from the source sensor nodes. The mathematical formulation of packet dropping probability rate is as given below.

$$PDPR = \frac{No.of\ packets\ \ dropped}{DP_s} * 100 \qquad (7)$$

From (7), the packet dropping probability rate '$PDPR$' is measured on the basis of data packets sent by the source sensor nodes 'DP_s'. It is measured in terms of percentage (%). Lower the packet dropping probability rate more effective the method is said to be.

Table 3 Tabulation for packet dropping probability rate

Data packets (KB)	Packet dropping probability rate (%)		
	RFIDD	DCIM	RMMP
9	71.35	78.92	84.16
18	63.27	70.47	76.51
27	66.14	73.34	79.38
36	69.16	76.36	82.40

45	72.37	79.57	85.61
54	75.14	82.34	88.38
63	68.32	74.52	80.56

In the experimental setup, the number of data packets ranges from 9 to 63. The results of seven simulation runs conducted to measure the packet dropping probability rate are listed in table 3. The packet dropping probability rate obtained using our scheme RFIDD offer comparable values than the state-of-the-art methods.

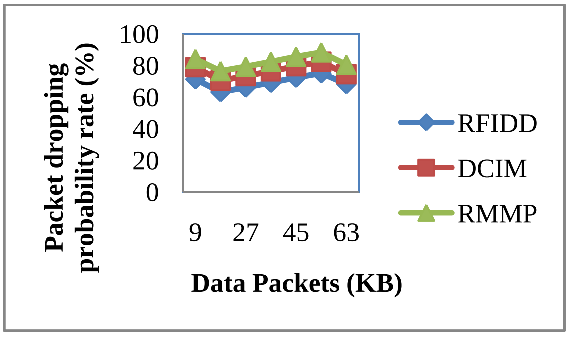

Figure 8 Measure of packet dropping probability rate

As shown in the figure 8, the packet dropping probability rate of three different schemes RFIDD, DCIM and RMMP are analyzed. The packet dropping probability rate is the ratio of number of packets dropped to the packets sent. It shows that using RFIDD scheme, when the number of data packets increases, the packet dropping probability rate first rises (9 data packets), then drops (18 data packets) and again rises (54 data packets). But using DCIM [1] and RMMP [2], comparatively increases packet dropping probability rate than that of the RFIDD scheme. This is because of the application of Observant Reasoning algorithm, optimal result is identified that it recognizes every packet dropping nodes in a significant manner. So that, compared to existing DCIM [1] and RMMP [2], RFIDD scheme reduces the packet dropping probability rate by 10.27% and 18.83%. This result shows that RFIDD scheme has the ability to sustain more number of data packets even for large node densities.

4.3 Impact of Security

Security with respect to data being collected is measured on the basis of data packets received at the base station in WSN. Therefore, security is the difference between the total packets sent to the packets not received at the base station.

$$S\,(DC) = DP_s - DP_{nr} \qquad (8)$$

From (8), 'DP_s' refers to the data packets (i.e. size) sent and 'DP_{nr}' refers to the data packets not received (i.e. size) at the base station in WSN. It is measured in terms of packets per second (p/s).

Table 4 Tabulation for data delivery security

Data packet size (KB)	Data delivery security (pps)		
	RFIDD	DCIM	RMMP
50	42	37	31
100	88	75	68
150	127	104	88
200	184	168	154
250	235	211	205
300	273	249	241
350	342	325	314

In table 4, data delivery security is compared for different sizes of data packets at the base station in WSN. The experiments were conducted using seven data packets with an average size of 350 KB and the data delivery security is measured in terms of packets per second (PPS).

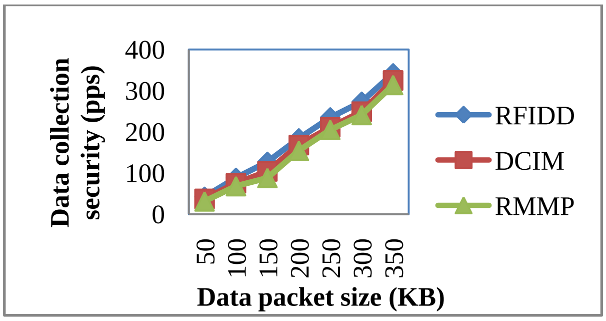

Figure 9 Measure of data delivery security

Figure 9 depicts the data delivery security with respect to several data packet sizes in the range of 50KB to 350KB. From the results shown in the figure, it is observed that the data delivery security is comparatively higher over the other methods. When compared to existing DCIM [1] and RMPP [2], the data delivery security of RFIDD scheme increases by 11.06% and 18.37%. Such experiments demonstrate that the data delivery security of RFIDD scheme is stable and has little impact with the increase in the size of data packet. This is because of the application of Adapted Key Management Routing (AKMR) protocol that performs the encryption, authentication and decryption process separately to attain higher security ratio on RFIDD scheme.

4.4 Impact of Average response time

The average response time in milliseconds (ms) is calculated as time taken to measure the average response, the product of number of nodes and the time taken to send the data packets from the source node to destination node. It is represented as follws,

$$RT = Number\ of\ nodes * Time\ (DP_{SN-DN}) \qquad (9)$$

Where number of nodes is the nodes processed by the system, 'DP_{SN-DN}' is the time for data packets to be sent from the source node 'SN' to the destination node 'DN' respectively.

Table 5 Tabulation for average response time

Number of nodes	Average response time (ms)		
	RFIDD	DCIM	RMMP
10	10.5	11.8	12.3
20	18.3	20.6	21.8
30	24.7	26.9	27.9
40	20.1	22.4	23.6
50	23.9	25.2	26.4
60	22.5	24.8	25.3
70	29.3	31.6	32.6

Table 5 shows the average response time with respect to 70 sensor nodes with a moving speed of 25 m/s. To better perceive the efficacy of the proposed RFID scheme, substantial experimental results are illustrated in Figure 10 and compared against the existing DCIM [1] and RMMP [2] respectively.

Figure 10 shows the impact of average response time with respect to varying sensor nodes in the range of 10 to 70 and the average response time using three methods differs according to the size of sensor nodes. The results reported above confirm that with the increase in the number of sensor nodes being sent to the base station, the average response time also increases. From figure 8, the average response time using three methods differs according to the size of sensor nodes.

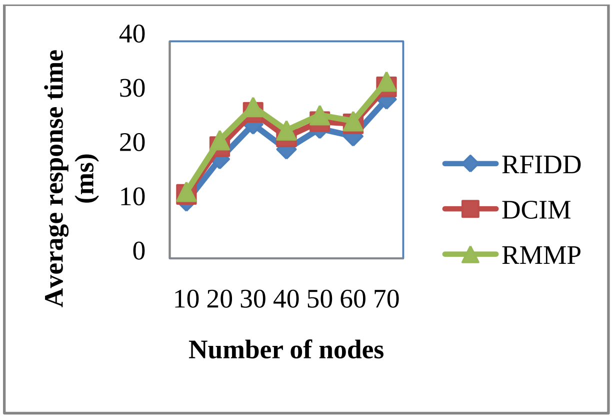

Figure 10 Measure of average response time

As illustrated in Figure, the proposed RFIDD scheme performs relatively well when compared to two other methods DCIM [1] and RMMP [2]. This is because of the application of three different keys, Pair Key, Sensor Node Base Key and Transmission Key that that perform secure communication between the source sensor and destination node in WSN. As a result, authentication is performed that in turn reduces the average response time of RFIDD scheme by 9.83% compared to DCIM and 14.40% compared to RMMP.

5. CONCLUSION

In this paper, by following the proposed effective data delivery on different network environments, a Routing Function Independent Data Delivery (RFIDD) Scheme is presented to improve the data delivery ratio and thus reduce the packet dropping probability rate in wireless sensor networks. An Observant Reasoning algorithm is proposed, which takes the advantage of identifying the concession nodes (i.e. packet dropping nodes) over wireless network into account. Next, by applying Adapted Key Management Routing (AKMR) protocol, the security while performing data delivery on wireless network is improved significantly. The correctness and complexity of the proposed scheme is shown and its performance is evaluated analytically. Simulations were conducted to measure the performance of RFIDD scheme and the performance is evaluated in terms of different metrics to perform data delivery at the base station in WSN that include data delivery ratio, packet dropping probability rate, average response time and security. The results show that RFIDD scheme offers better performance with an improvement of security by 14.71% and reducing the average response time by 12.11% compared to DCIM and RMMP respectively. The future scope of this proposed work will concentrate on implementing novel algorithm to improve data delivery ratio.

6. ACKNOWLEDGMENTS

The authors thank the anonymous reviewers who provided useful feedback that helped improve the quality of this paper.

7. REFERENCES

[1] Fawaz, K. and Artail, H. 2013. DCIM: Distributed Cache Invalidation Method for Maintaining Cache Consistency in Wireless Mobile Networks, IEEE Transactions on Mobile Computing, Volume 12, Issue 4, pp. 680-693.

[2] Al-Hamadi, H. and Chen, I.R. 2013. Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks, IEEE Transactions on Network and Service Management, Volume 10, Issue 2, pp.189-203.

[3] Vasserman, E.Y. and Hopper, N. 2013. Vampire attacks: Draining life from wireless ad-hoc sensor networks, IEEE Transactions on Mobile Computing, Volume 12 Issue 2, pp.318-332.

[4] Yang, S., Yeo, C.K., and Lee, B.S. 2012. Toward Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks, IEEE Transactions on Mobile Computing, Volume 11, Issue 1, pp. 111-124.

[5] Cui, T., Lu, F., Sethuraman, V., Goteti, A., Subramanya, P., Rao, N., and Subrahmanya, P.2011. Throughput Optimization in High Speed Downlink Packet Access (HSDPA), IEEE Transactions on Wireless Communications, Volume 10, Issue 2, pp. 474-483.

[6] Yu, Z. and Guan, Y. 2010. A Dynamic En-route Filtering Scheme for Data Reporting in Wireless Sensor Networks, IEEE/ACM Transactions on Networking, Volume 18, Issue 1, Pages 150-163.

[7] Parvez, N., Mahanti, A., and Williamson, C. 2010. An Analytic Throughput Model for TCP NewReno, IEEE/ACM Transactions on Networking, Volume 18, Issue 2, pp. 448-461.

[8] Starobinski, D. and Xiao, W. 2010. Asymptotically Optimal Data Dissemination in Multichannel Wireless Sensor Networks: Single Radios Suffice,

IEEE/ACM Transactions on Networking, Volume 18, Issue 3, pp. 695-707.

[9] Dang, H. and Wu, H.2010. Clustering and Cluster-Based Routing Protocol for Delay-Tolerant Mobile Networks, IEEE Transactions on Wireless Communications, Volume 9, Issue 6, pp. 1874-1881.

[10] Dai, R., Wang, P., and Akyildiz, I.F.2012. Correlation-Aware QoS Routing With Differential Coding for Wireless Video Sensor Networks, IEEE Transactions on Multimedia, Volume 14, Issue 5, pp. 1469-1479.

[11] Wan, Z., Ren, K., and Gu, M. 2012. USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks, IEEE Transactions on Wireless Communications, Volume 11, Issue 5, pp. 1922-1932.

[12] Choi, B., Wong, T.F., and Shea, J.M .2012. Geographic Transmission with Optimized Relaying (GATOR) for the Uplink in Mesh Networks, IEEE Transactions on Wireless Communications, Volume 11, Issue 6, pp. 2095-2105.

[13] Alia, O.M 2014. A Decentralized Fuzzy C-Means-Based Energy-Efficient Routing Protocol for Wireless Sensor Networks, Hindawi Publishing Corporation, The Scientific World Journal, Volume 2014, pp. 1-10.

[14] Wang, S., Basalamah, A., Kim, S.M., Guo, S., Tobe,Y., and He, T . 2015. Link-Correlation-Aware Opportunistic Routing in Wireless Networks, IEEE Transactions on Wireless Communications, Volume 14, Issue 1, pp. 47-56.

[15] Sheikholeslami, F., Nasiri-Kenari, M., and Ashtiani, F. 2015. Optimal Probabilistic Initial and Target Channel Selection for Spectrum Handoff in Cognitive Radio Networks, IEEE Transactions on Wireless Communications, Volume 14, Issue 1, pp. 570-584.

[16] Zhou, Y. and Zhuang, W .2015. Throughput Analysis of Cooperative Communication in Wireless Ad Hoc Networks With Frequency Reuse, IEEE Transactions on Wireless Communications, Volume 14, Issue 1, pp. 205-218.

[17] Yaoa, L., Deng, J., Wanga, J., Wu, G. 2015. A-CACHE: An anchor-based public key caching scheme in large wireless networks, Elsevier, Computer Networks, Volume 87, pp. 78–88.

[18] Diaz, J.R., Lloret, J., Jimenez, J., Sendra, S., and Rodrigues, J.P.C. 2014. Fault Tolerant Mechanism for Multimedia Flows in Wireless Ad Hoc Networks Based on Fast Switching Paths, Hindawi Publishing Corporation, Mathematical Problems in Engineering, Volume 2014, pp.1-13.

[19] Lee, H.J. 2014. Greedy Data Transportation Scheme with Hard Packet Deadlines for Wireless Ad Hoc Networks, Hindawi Publishing Corporation, The Scientific World Journal, Volume 2014, pp. 1-9.

[20] Shen, H., Bai, G., Zhao, L., and Tang, Z .2012. An Adaptive Opportunistic Network Coding Mechanism in Wireless Multimedia Sensor Networks, Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2012, pp. 1-14.