VARIANCE AWARE SECURE ROUTING FOR HETEROGENEOUS WIRELESS SENSOR NETWORKS

***Kamal Kumar*[1], *A. K. Verma*[2], *R.B. Patel*[3]**

[1]M.M.Engineering College, Mullana, Ambala-133207,India
[2]Thapar Universty, Patiala-147004, India
[3]D.C.R.. Univerity of Science and Technology, Murthal, Sonepat-131039,India
kamalkumar.cse@mmumullana.org, akverma@thapar.edu, patel_r_b@yahoo.com

ABSTRACT

Secure Communication is important parameter in unattended and hostile environment. Wireless Sensor Networks (WSNs) are deployed and operate in vulnerabilities and are candidate networks which should be commissioned for security provisioning in end to end communications. Because of their specialized applications many solutions in terms of cryptographic, Intrusion Detection and Key Management have been proposed. Most solutions lack and seem of ignoring the fact that route is as strong as weakest link in the route with respect to other links in the route. Variance of number of keys and high average number of keys on routes is an issue that we tried to resolve in our proposal using non-uniform key pre-distribution in Heterogeneous Wireless Sensor Networks (HWSNs). Analytical and Simulation based study supports our concern and reports an improvement in Average number of keys in almost 60 percent routes and decreasing variance in almost 50 percent routes in random and probabilistic neighbourhood.

Keywords: Metric, Variance, Communication, Heterogeneous.

1.0 INTRODUCTION

Wireless Sensor Networks (WSNs) are known for their reliability, accuracy, flexibility, and ease of deployment; as a result they are being widely used for various monitoring systems, data collection, and process control applications [5]. Because of the small size, limited processing power, and unattended deployment of individual sensor nodes, they are greatly prone to security compromises. Thus, one concerned issue when designing wireless sensor network is the routing protocol that requires the researchers to provide as much security to the application as possible. Therefore, it is important to build security within the network architecture and protocols, so that a WSN can successfully operate in the presence of component failures or malicious attacks or both [4].

Traditional security protocols are not applicable for resource constrained unattended distributed environment. Secure routing in WSNs presents challenges due to low computing power, small memory, limited bandwidth, and especially very limited energy. Many Denial-of-Service (DoS) attacks, which are the result of any action that prevents any part of a WSN from functioning correctly or in a timely manner, can be easily employed against routing in WSNs.

In this paper we propose variance aware routing tree rooted at Base Station (BS) and is based on the recognized GPSR [16]. The proposed prototype uses key pre-distribution in heterogeneous wireless sensor networks for establishing key paths for secure routes. We are able to establish routes in the network which takes care of variance in average number of keys of links on a route from node to sink. Our protocol is driven to a challenge and concept that route is as strong as the weakest link in the route. It is believed that reducing variance in number of keys of links will enable to choose paths on which keys in links are close to average number of keys on the path from node to sink. Thus contributions of our work includes, variance controlled resilient paths and loop avoidance. The paper is organized in section 1 introducing the problems undertaken and solution approach. Section 2 refers related work with section 3 and 4 describing networks model and our proposal. Section 5 discusses analytical modelling, with section 6 discusses simulation and performance. Section 7 discusses an application with section 8 finally concludes the work.

2.0 RELATED WORK

Key management is a fundamental challenge in a large-scale and resource-limited sensor network. A number of pair-wise symmetric key establishment schemes [7], [8], [9], [10], [13], [14], have been recently proposed. Most of them use the idea of probabilistic key sharing [10] to establish trust between two nodes, each with different emphasis on enhanced security protection [7], flexibility of security requirements, high probability of key establishment and reduced overhead [13], or utilization of deployment knowledge [4]. Such pair-wise keys can be used to authenticate a node's identity or messages; however, issue of weakest link on the route from node to sink cannot be avoided. Semantic verification of the data becomes necessary to detect any fabrication attacks.

Secure routing has been extensively studied in the context of ad-hoc networks [6], [12], [11], [15]. However, none of these protocols can be applied in sensor networks, because none addresses the unique feature of data-centric communication, and the network scale is limited by the excessive number of keys each node should store. The challenges of secure sensor routing are discussed in [17], together with security threat and counter-measurement analysis on a few popular routing protocols. However, it does not consider the issue of resilience of member links on the route from node to sink. Most of the security solutions are routing after but none has considered security before routing. We addressed the issue of resilient routes in the WSN in our work. Work in [3] addresses the issue of end-to-end security based on location but don’t address the issue of high variance of resilience of the participating links.

3.0 NETWORK ELEMENTS AND NETWORK MODEL

Our focus on is large-scale HWSNs with the flat architecture. *SNs* are divided into two categories; namely H-Sensors and L-Sensors. H-Sensors are small number of *SNs* possessing higher memory, transmission range, multiple transmission ranges, processing power and battery life. Our network model has two different kinds of wireless devices on the basis of functionality; sink node/base station (BS) and sensor node (SNs) .

3.1 Network Elements

Our focus on is large-scale HWSNs with the flat architecture. *SNs* are divided into two categories namely H-Sensors and L-Sensors. Our network model has two different kinds of wireless devices on the basis of functionality; sink node/base station (BS) and sensor node (SNs) .

- Sensor node (SNs)**:** Sensor nodes are new generation L-Sensors which are inexpensive, limited-capability, generic wireless devices. Each *SN* has limited battery power, memory size, data processing capability and short radio transmission range. *SNs* Communicate with its neighbour *SNs* and *BS* . H-Sensors are small number of *SNs* possessing higher memory, larger transmission range, multiple transmission ranges, higher processing power and battery life.

- Sink node/Base station (BS) **:** Sink node is the most powerful node in a WSN, it has virtually unlimited computational and communication power, unlimited memory storage capacity, and very large and powerful radio transmission range which can reach all the *SNs* in a WSN. Sink node can be located either in the centre or at a corner of the network based on the application. For our proposal *BS* is situated at random location in deployment area.

3.2 Network Model

In our network model, a large number of *SNs* are randomly distributed in an area. *BS* takes charge of the whole network’s operation. *SNs* monitor the surrounding environment and transmit the sensed readings to their respective *BS* via multi-hop relay path. Nodes are deployed randomly in the field. *BS* is situated at random location in deployment area. *BS* can reach any node in the deployment area directly is presumed. Each sensor has small radius of transmission i.e. r . Nodes are static and battery cannot be replaced or charged after deployment.

4.0 NETWORK INITIALIZATION

In an effort to achieve avoidance approach for secure communication we proceed in two steps namely: Key Management Scheme for Heterogeneous Wireless Sensor Networks and Security Aware Route Establishment in GPSR [16]. Routing and key management go hand in hand and cannot be distinguished from each other. Table 1 lists the parameters in protocol with description and their notations.

4.1 Key Management

Key management scheme is divided into multiple stages namely; Key Pre-Distribution, Pair-Wise Key Establishment and Establishing Routing Paths.

4.1.1 Key Pre Distribution

We considered WSN with N sensor nodes and a BS . N Sensor nodes are divided into two classes namely L-Sensors and H-Sensors, and respectively have n_1 and n_2 nodes. We then pre-distribute k_1 and k_2 unique keys such that $k_1 \leq k_2$ chosen from a large key pool with size K respectively to L-Sensor and H-Sensor. Sink is pre-distributed with all K keys but uses only k_2 keys similar to H-sensor from key pool. After this, the sink is deployed at any random position, similar to other nodes of WSN.

For each of H-Sensor node, k_2 unique keys are chosen randomly from the key pool with replacements. L-Sensors are distributed k_1 keys from key pool.

Table 1: Notations Used

Symbols Used	Exploits
n_2	Number of H-Sensors
K	Key Pool Size
N_c	Number of Captured Nodes
N	Number of Nodes
k_1	Keys Allotted to L-Sensors
k_2	Keys Allotted to H-Sensors
n_1	Number of L-Sensors
c	Number of Classes

4.1.2 Pair-Wise Key Establishment

Having obtained keys and key-IDs of pre-distributed keys SNs now wait for a beacon from BS . This beacon is initiation of two-way key paths establishment. Both $SN - BS$ and $BS - SN$ paths are established as a result. This support is exploited for supporting both push-pull paradigms of communication. TTL (Time-to-Live) of beacons is set to 1 .i.e. $TTL = 1$. All one-hop neighbours compute an illusionary resilience towards BS . This value if denoted by IR (Illusionary Resilience) and equals sum of IR_{sender} and the square of number of pre-distributed keys shared with the sender of beacon. As nodes away from BS will receive multiple beacons informing sender's IRs ; nodes locally select one of sender as next hop towards BS for which equation (1) gives maximum. Receiving nodes wisely select a sender as their next-hop towards BS on the basis of following equation.

$$IR_j = max\left\{IR_k + \left(K_{comm}\left(j,k\right)\right)^2\right\} \qquad (1)$$

If any node j has received IR values from p distinct one hop neighbours then $k = 1..p$. $K_{comm}\left(j,k\right)$ Denote the number of pre-distributed keys that a node j shares with k^{th} sender among p distinct sender neighbours. If any node i shares one or more pre-distributed keys with any one-hop neighbour j, then there is one direct key path with one hop between them. For routing purposes selection of forwarder towards BS is informed to concerned node. Having completed the process of computing IRs towards BS nodes gets arranged like a tree rooted at BS .

5.0 ANALYTICAL MODELLING AND EVALUATION

As per non-uniform key pre-distribution scheme that we used H-Sensors are given more number of keys than L-Sensor Keys. Possibility of sharing more keys with H-Sensors is high compared to that of L-Sensors. This result in next hop of any random node j in (1) towards BS possibly is H-Sensor. Process of computing IR continues until all the nodes in network have computed IRs toward BS . At the end of route establishment; nodes are aware of which of one-hop neighbours will route information through them. We can compute the probability of sharing common keys with node. The resilience of any link between i and j is dictated by number of protection keys and subsiding cases of no-common keys. Key paths can be constructed between any node i and node j by sending a request to its neighbours, containing the node IDs of i and j . In our proposal this is obtained while constructing routing tree. After a neighbouring node j receives the IR_i as well as key IDs of all the pre-distributed keys of i^{th} node; j can checks if it shares pre-distributed keys with node i . Node j prefers to use all the common keys for one-hop direct key path between i and j .

Node j sends an acknowledgement back to node i with which node j shares maximum number of keys and proceeds to compute own IR . In this way, a one-hop key path $i - j$ is constructed. After node i constructs one-hop key path to node j , messages are encrypted or decrypted on hop by a combination (e.g., XOR) of all shared keys on that hop. Ultimately, the pair-wise key between nodes i and j is a combination of all the common keys. Nodes must store the number of protection keys for each link. Assuming that $K\left(i\ ,j\right)$ denote the number of shared keys between i and j . The number of protection keys between i and j is exploited by $P_r\left(i\ ,j\right)$ and is defined as follows.

$$P_r\left(i\ ,j\right) = K\left(i,j\right) \qquad (2)$$

Not to forget that some of the protection keys between a pair of nodes is maximum possible common keys. With no confusion we conclude that at the most one link is set between a pair of nodes.

5.1 Analytical Performance Evaluation

We assume the number of captured nodes $\left(N_c\right)$ is known. Nodes at any distance can reach the sink in at most $N-1$ hops and will be able to avoid any loop as routing tree is spanning tree rooted at BS . For a specific communication from any random node to sink with h hopes probability can be expressed as $RES\left(h\right)$ and is the end to end resilience for a path with h hops. In (3), $RES\left(h\right)$ is calculated as product of probabilities that all nodes and links are un-captured /uncompromised in the path with h hops. Then we have,

$$RES\left(h\right)=\frac{\binom{N-h}{N_c}}{\binom{N}{N_c}}RES_{link}{}^{h} \qquad (3)$$

In (3) RES_{link} is the resilience of link and in-fact is probability that a link between two un-captured nodes is uncompromised. In (3), the value of $\frac{\binom{N-h}{N_c}}{\binom{N}{N_c}}$ is probability of ways in which node can be captured provided none of nodes in h hopes used for communication is captured. Our tree construction mechanism which is distributed in nature and proceeds breadth-first way uses underlined pre-distribution to increase the value of RES_{link}.

Computation of SEL_i : Before we can calculate the value of RES_{link} we define the probability value SEL_i which is the probability that a node on the path between a sensor and the sink is either of i (L or H Sensor) class. Nodes get linked to active routes which results in maximizing of equation (1). Derivation of SEL_i will follow after computation of $p_{common}\left(i,j,l\right)$ which is defined as the probability of any i class sensor node shares l keys with a j class sensor node.

Consider p_i as percentage of class i nodes in the network and is given by $p_i = {n_i}/{N}$. If $P_{common}\left(i,j,l\right)$ denotes the probability that any i class sensor node shares l keys with a j class sensor node given that nodes are one hop neighbours. The equations are as under:

$$p_{common}\left(i,j,l\right)=\binom{K}{l}\frac{\binom{K-l}{K_i}}{\binom{K}{K_i}}\frac{\binom{K-K_i}{K_j-l}}{\binom{K}{K_j}} \qquad (4)$$

If $P_{prefer}\left(j,l\right)$ is defined as the probability of class j node is preferred over class l node as next-hop on routing path, the equation for $P_{prefer}\left(j,l\right)$ can be defined as follows:

$$P_{prefer}\left(j,l\right)=\sum_{j=1}^{2}\left(\sum_{u=1}^{\min\{k_i,k_j\}}P_{common|\mathrm{P}_{parent}=\left(IR_j+u^2\right)}\left(i,j,\mathrm{u}\right)*\left(\sum_{v=1}^{\min\{k_j,k_l\}}P_{common|P_{parent}\le\left(IR_m+v^2\right)}\left(i,l,v\right)\right)\right) \qquad (5)$$

$P_{parent}=\left\{min\left\{IR_j+u^2\right\}\quad|\,j=1..p\right\}$ Where; u subset of pre-distributed keys.

Finally, the expression of SEL_i is as given by where $f\left(j\right)$ equals 1 when $i=j$, otherwise 0.

$$SEL_i=\binom{p}{1}*\left(\prod_{j=1}^{2}\left(P_{prefer}\left(i,j\right)\right)^{p*P_i-f\left(j\right)}\right) \qquad (6)$$

In (8), p is the average number of nodes from which node receives IR values.

Derivation of RES_{link} Given the expressions of SEL_i as in (6) we uses the expression for RES_{link} in this section where denote $RES_{link}(i,j)$ is resilience of the pair-wise key between a node of i class and j class node:

$$RES_{link} = \sum_{i=1}^{2}\sum_{j=1}^{2} SEL_i * SEL_j * RES_{link}(i,j) \quad (7)$$

Where expressions for $RES_{link}(i,j)$ is as follows:

$$RES_{link}(i,j) = 1-\left(1-P_{res}\left(K_{avg}(i,j)\right)\right) \qquad (8)$$

Where $P_{res}(i)$ is the probability that at least one of i unique pre-distributed keys is not disclosed to the attacker, $K_{avg}(i,j)$ as the average number of shared pre-distributed keys between a class i node and a class j node, $K_{avg}(i)$ as the average number of shared pre-distributed keys between a class i node and one of its physical neighbours. In (8) $P_{res}\left(K_{avg}(i,j)\right)$ is probability that the direct one-hop key path between a class i node and a class j node is uncompromised. We now derive the expressions for $P_{res}(i)$, $K_{avg}(i,j)$ and $K_{avg}(i)$. Given the number of captured nodes N_c , the average number of disclosed pre-distributed keys, denoted by K_{dis} is given by,

$$K_{dis} = \left(1-\left(1-\frac{K_{avg}}{K}\right)^{N_c}\right) \qquad (9)$$

Where; K_{avg} is the average number of keys pre-distributed in sensor nodes. The expression of K_{avg} is given by,

$$K_{avg} = \sum_{i=1}^{2} p_i \times k_i \qquad (10)$$

Given the expression of K_{dis} above, we are able to give the expression of $P_{res}(i)$ as,

$$P_{res} = 1-\frac{\binom{K-i}{K_{dis}-i}}{\binom{K}{K_{dis}}} \qquad (11)$$

Recall the expression of $P_{comm}(i,j,l)$ in (4) above, the expressions of $K_{avg}(i,j)$ and $K_{avg}(i)$ can be given by,

$$K_{avg}(i,j) = \sum_{l=1}^{\min\{k_i,k_j\}} l \times P_{common}(i,j,l) \qquad (12)$$

$$K_{avg}(i) = \sum_{j=1}^{c} p_j \times K_{avg}(i,j) \qquad (13)$$

There is no possibility of loops as routes are maintained as tree. Selection of parent towards BS is governed by equation (5). Only one of potential parents will be announced parent of any node.

We have considered the quality and are not quantity of resilience. Resilience is defined as probability of not disclosing when compromised. Resilience of routes depends upon resilience of links on the route. Equation (3) above quantify the resilience of routes. Further resilience of link depends upon the number of keys in the link used for encryption and decryption and can be concluded from equation (8). We have proposed equation (5) to prioritize one node over another while routes are being built. Here we try to select the node if it maximizes the value for equation in (1) in section 4. We have modified preference criterion from [2]. This preference criterion is modification with a view that node on the routes should do minimum damage to the quality or quantity of resilience. This may lead to an increased path lengths of some of the routes but without compromise in our QoS i.e. resilience. As resilience is dictated by the number of keys in the links we focussed to quantify only improving in average keys on the routes although we are increasing path lengths in some routes.

We have listed few equations from [2] to maintain correlation. We are able to establish the reduction in variance in resilience of the links being added to routes being built. The simulation based validation strengthens our proposal where we proved to increase the average number of keys on the routes and reduce the variance in number of keys simultaneously which according to our knowledge is not considered by any earlier work.

6.0 SIMULATION AND PERFORMANCE DISCUSSION

In an effort to realize the effect of our next-hop selection method we established a simulation environment using MATLAB. Our focus is to prove that our mechanism is able to bring an improvement in number of keys in links on routes if alternates are available and reduce the variance in number of keys on links on the routes. Validating this fact validates that there will be a definite improvement in resilience on routes from node to sink. The almost ignored fact that route is as resilient as the weakest link is taken care of. A major contribution of our work is to decrease the variance in resilience on routes. This will overall increase the resistance against capture attacks. In our case, the range of variation in resilience of member links in a path is limited by our next hop selection method. We categorically chose a node as our parent in routing tree construction which minimizes the variation in the IR value of newly added link with respect to already existing links on the paths. The most common way to describe the range of variation is standard deviation or variance (usually denoted by the Greek letter sigma: σ).

6.1 Simulation Setup

We simulated a simple scenario where routes are formed using GPSR [16] using geographic distance as metric of concern. In other case we considered key-shares between nodes as their distance metric. A node i is next hop for node j if i shares more key with j compared to other nodes. GPSR under non uniform key distribution scheme finds routes form sink to nodes with effort to maximize keys on the routes between sink and nodes. Finally we simulated GPSR under non uniform key management using IR values as the distance which tries to maximize the keys in the routes as well limits the variance in number of key values on the routes. We considered following values for various protocol parameters $c = 2$, $k_1 = 45$, $k_2 = 60$, $N = 45$, $n_1 = 30$, $n_2 = 15$ and $K = 1000$.

The network to be studied is deployed in 100x100 area with transmission range = 19. We have considered two classes of nodes and deployment of nodes is as shown in Fig. 1.

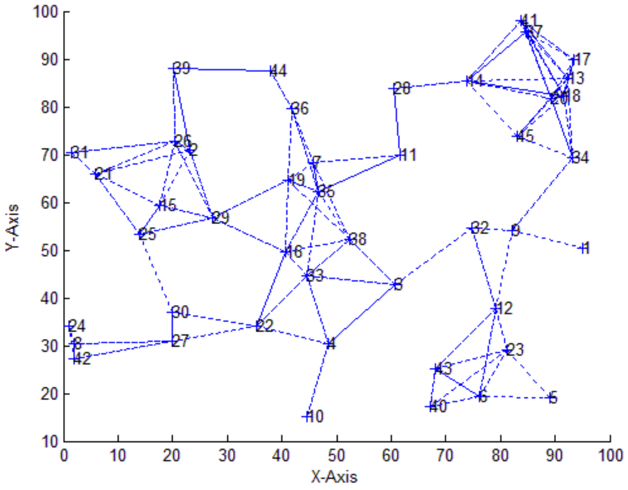

Fig. 1. Random Deployment of Nodes in 100*100

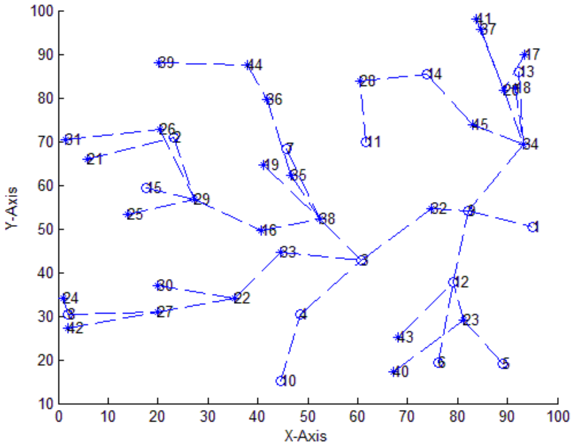

Fig. 2. Routing Tree in GPSR

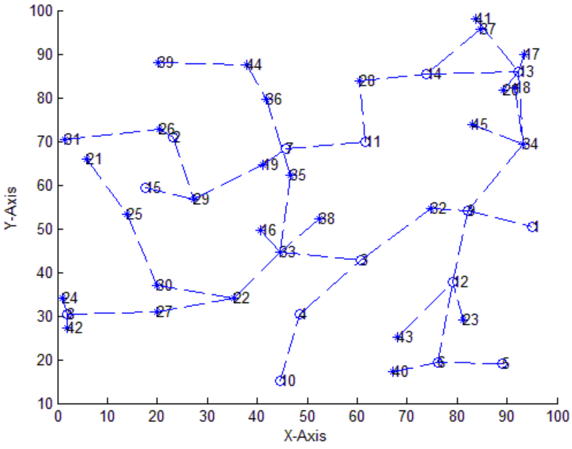

Fig. 3. Routing Tree in GPSR under Non-uniform key distribution

In figs. above; routes in three scenarios are differing from others to some extent as per distance metric. It must be understood that next-hop nodes are limited by the neighbourhood. This limitation is even more pronounced in keyed paths. The graph in Fig. 5 exhibits a comparison of route lengths in three different scenarios. The average keys on routes from nodes are shown in Fig. 6 under non uniform and variance conscious non uniform keyed paths. In Fig. 7 we have shown the variance in keys values on the routes in GPSR under non-uniform and variance conscious scenarios. Visibly the variance in our proposal for secure version of GPSR has reduced in most of the cases under neighbourhood limitation in random key distribution environment. The variance in keys values for hops on each route is computed as is given in Fig. 7.

6.2 Performance Discussion

The resilience of any path is determined by the resilience of the weakest link. There is huge possibility that newest link added to the route is weakest with respect to resilience of the route being formed. This weakest link decides the resilience of the route. In our proposal we defined a value IR which should be minimized while adding a new link on any route. The mathematical modelling and graphs above validate our concern and we tried and successfully tried to bring down the variation in the key values in the links. It is perceived in many works that next-hop selection should add maximum possible keys to total keys in the route, but simulation of such scenarios revealed that it may result in adding some link which is weaker with respect to links already added.

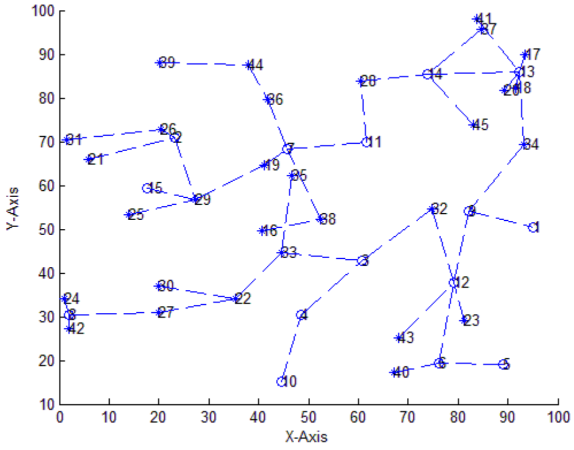

Fig. 4. Routing Tree in GPSR under VARIANCE non uniform key distribution

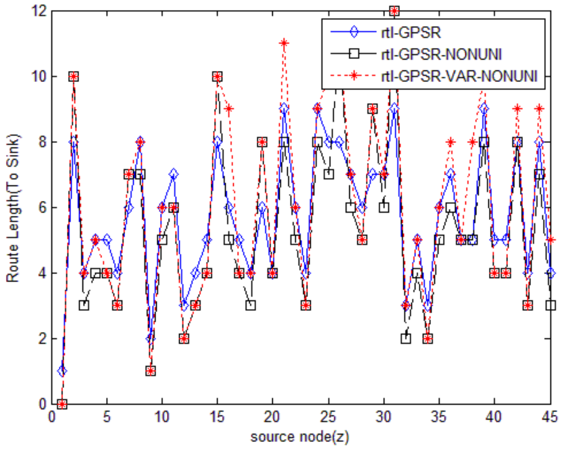

Fig. 5. Route lengths comparison in GPSR under three scenarios.

Graph in Fig. 6 reveals that average keys on the routes under such perception is not always the highest possible. This perception is even challenged by our results on route lengths in Fig. 6. Route lengths under such perception are smaller than our proposal but reduced or smaller routes should have more average number of keys on routes. Our proposal has increased the route lengths in most of the cases and simultaneously improved values of average keys on the routes. If average keys on routes considered as quality or quantity of resilience then we improved upon that. Going further we brought down the variance in resilience of new links being added. The comparison in variance of keys on routes is plotted against the perceptions in literature in Fig. 6 and if it was possible we are able to reduce variance in limitation posed by neighbourhood.

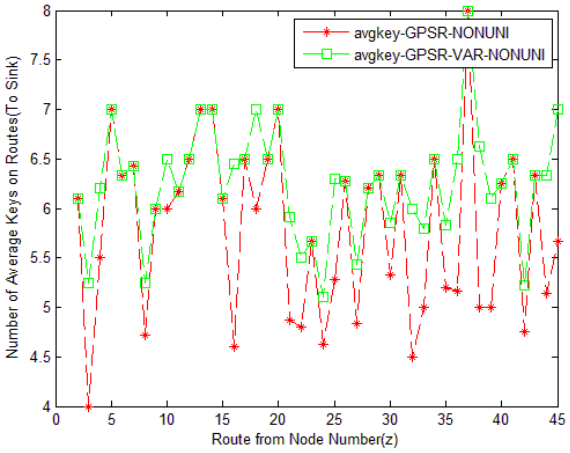

Fig. 6. Comparison of average keys on routes in GPSR Keys on GPSR NONUNIFORM and GPSR-VAR-NON-UNIF-distribution ORM Key distribution

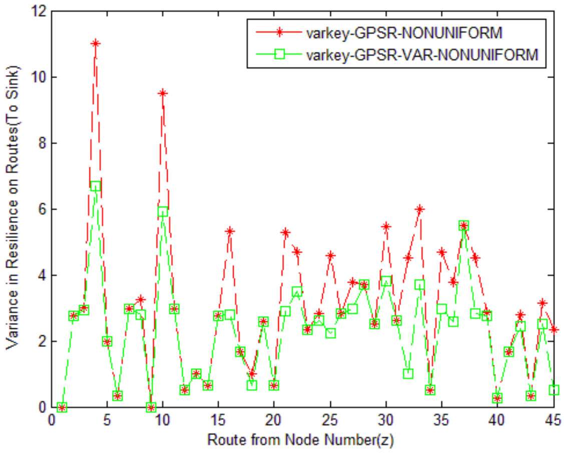

Fig.7. Comparison of variance in number of routes in GPSR-NON-UNIFORM Key and GPSR-VAR-NON-UNIFORM Key distribution

7.0 AN APPLICATION: ROUTING INFRASTRUCTURE

Traffic patterns in data-centric routing protocols are generally event's query-reply based. In our proposal selection of a forwarder node towards *BS* is informed back by selector and this would help nodes build their selector or children down the tree. Our selection criteria given in (1) and (5) for non-uniform key distribution scenario has improved the possibility of many nodes linking to the node which minimize (1) and thus gets selected as forwarder nodes towards BS. We are not subsiding the possibility of L-Sensors gets selected as forwarder node. As forwarders nodes are forwarders for multiple *SNs* thus forwarders are called Traffic Mergers Points (TMPs). TMPs can build a set of selector nodes. At the end nodes are classified as TMPs or non-TMPs. As some of selectors of TMPs are TMPs down the tree and other non-TMPs. Our routing tree gets converted into a tree where non-leaf nodes are working as TMPs and leaves are working as non-TMPs.

7.1 Reduced Broadcast

Any query from *BS* is a broadcast from *BS* and will be received by nodes one-hop away from *BS*. There are many possibilities with reference to response at node. These are as follows:

- If receiving node is non-TMP and can reply the query; without retransmission of query a reply will be forwarded through its TMP toward *BS*.
- If receiving node is TMP and can reply the query; without retransmission of query a reply will be forwarded through its TMP toward *BS*.
- If receiving node is a TMP and can't reply then node should broadcast query to all its Children.
- If query is received by non-TMP and is not able to reply the query will not be forwarded and is dropped silently.

A query will reach every such node who can reply; without retransmission of query by non-TMPs and broadcast by TMPs only. None of the node received multiple copies of query. A detailed operation of routing protocol is investigation and along with performance modeling using analytical techniques.

8.0 CONCLUSION

In this paper, we address the issue of providing variance controlled resilient paths from nodes to sink, via non uniform key pre-distribution. The routes got longer in effort to achieve variance controlled keyed paths but without lowering and even increased the average keys in most routes. The analytical modelling is validated well with the help of simulation of proposal and effects are evaluated using GPSR. Both theoretical analysis and simulations validate the strength of our approach.

REFERENCES

[1] P. Traynor, H. Choi, G. Cao, S. Zhu, and T. L. Porta, “Efficient Hybrid Security Mechanism for Heterogeneous Sensor Networks”, *IEEE Transactions on Mobile Computing*, Vol. 6, No. 6, June 2007.

[2] Gu W., N. Dutta, S. Chellappan and X. Bai., “Providing End-to-End Secure Communications in Wireless Sensor Networks”, *IEEE Transaction on Network and Service Management*, Vol. 8, No. 3, September 2011, pp. 205-218.

[3] K. Ren, W. Lou, and Y. Zhang, “LEDS: Providing Location-Aware End-to-End Data Security in Wireless sensor networks", *IEEE Transaction Mobile Computing*, Vol. 7, No. 5, May 2008, pp. 585-598.

[4] T.V. Dam and K. Langendoen, “An adaptive energy-efficient MAC protocol for wireless sensor networks”, in *Proceedings of ACM international conference on embedded networked sensor systems (SenSys)*, 2003.

[5] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless Sensor Networks: A Survey”. *IEEE Computer Networks*, Vol. 38, No. 4, March 2002, pp. 393-422.

[6] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, “An On-Demand Secure Routing Protocol Resilient to Byzantine Failures”, in *Proceedings of the 1st ACM workshop on Wireless security* (WiSE '02), ACM, New York, NY, USA, pp. 21-30, 2002.

[7] H. Chan, A. Perrig, and D. Song, “Random Key Predistribution Schemes for Sensor Networks”, *In Proceedings of the 2003 IEEE Symposium on Security and Privacy (SP '03),*Washington, DC, USA, pp.197, 2003.

[8] R.G. Raj, V. Balakrishnan. “A Model for Determining The Degree of Contradictions in Information”. Malaysian Journal of Computer Science, 2011, 24(3): 160 – 167.

[9] W. Du, J. Deng, Y Han, and P. Varshney, “A Pairwise Key Predistribution Scheme for Wireless Sensor Networks,” In *Proceedings of the 10th ACM conference on Computer and communications security* (CCS '03), ACM, New York, USA, pp. 42-51.

[10] L. Eschenauer and V. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” in *Proceedings of ACM Conference on Computer and Communications Security (ACM CCS),* Washington DC, pp. 41-47, 2002.

[11] Y.C. Hu, D.B. Johnson and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad-hoc Networks," in *Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02)*, pp. 3-13, 2002.

[12] Y.C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks,” In *Proceedings of the 8th annual international conference on Mobile computing and networking* (MobiCom '02). ACM, New York, USA, pp. 12-23, 2002.

[13] D. Liu and P. Ning, “Establishing Pairwise Keys in Distributed Sensor Networks,” in *Proceedings of the 10th ACM conference on Computer and communications security (CCS '03),* ACM, New York, USA, pp. 52-61, 2003.

[14] D. Liu and P. Ning, “Location-Based Pairwise Key Establishments for Relatively Static Sensor Networks,” in *Proceedings of ACM Workshop on Security in Ad Hoc and Sensor Networks*, ACM, NEW YORK, USA, pp. 72-82, 2003.

[15] P. Papadimitratos and Z. Haas, “Secure Routing for Mobile Ad Hoc Networks,” in *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002),* San Antonio, TX, January 27-31, 2002.

[16] Karp B. and Kung H. T., “GPSR: greedy perimeter stateless routing for wireless networks”, in *Proceedings of the 6th annual international conference on Mobile computing and networking (MobiCom '00),* ACM, New York, NY, USA, pp. 243-254.

[17] Chris Karlof and David Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” in *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Application* , 11 May 2003, pp.113-127.

BIOGRAPHY:

Kamal Kumar received his M. Tech. as well as B. Tech degree from Kurukshetra University, Kurukshetra, India. Presently he is working as Associate Professor in Computer Engineering Department in M.M. Engineering College, Ambala, India. He is pursuing Ph. D from Thapar University, Patiala, India.

A. K. Verma is currently working as Associate Professor in the department of Computer Science and Engineering at Thapar University, Patiala in Punjab (INDIA). He received his B.S. and M.S. in 1991 and 2001 respectively, majoring in Computer Science and Engineering. He has worked as Lecturer at M.M.M. Engineering College, Gorakhpur from 1991 to 1996. His research interests include wireless networks, routing algorithms and securing ad hoc networks.

R. B. Patel received a PDF, Highest Institute of Education, Science & Technology (HIEST), Athens, Greece, 2005. He received a PhD in Computer Science and Technology from Indian Institute of Technology (IIT), Roorkee, India. He is member IEEE, ISTE. His current research interests are in Mobile and Distributed Computing, Security, Fault Tolerance Systems, Peer-to-Peer Computing, Cluster Computing and Sensor networks.