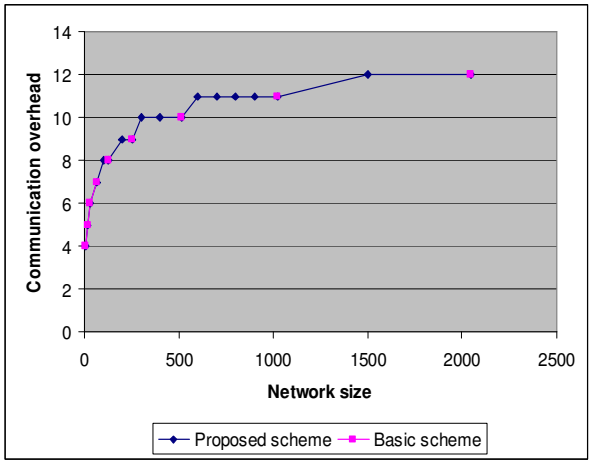

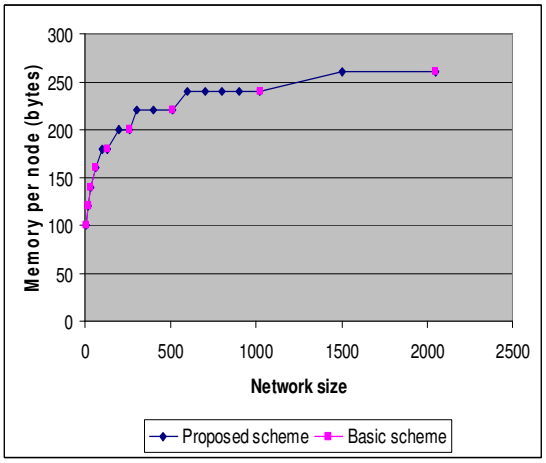

Figure 2 : Communication overhead vs. network size **Figure 3: Memory requirement vs. network size**

VI. CONCLUSIONS

A simple algorithm for generating an optimally-balanced complete hash tree is proposed in this paper. Given any number of leaf nodes, the algorithm builds a binary tree. Through mathematical analysis it is shown that the leaf nodes of the generated tree exists only on last and second-last level. Hence, it is concluded that such a tree is optimally-balanced complete hash tree. The complexity and memory requirement of the algorithm is $O(n)$ and it does not demand to represent the nodes in polynomial form to construct the tree. Experimental results show that, when the proposed algorithm is used for public key authentication in MANET; the AP and per node memory requirement remains optimal even though the number of leaf nodes are not of the order of power of two.

REFERENCES

[1] R. C. Merkle, "Protocols for Public Key Cryptosystems," in *Proc. IEEE Symposium on Research in Security and Privacy, 1980*.

[2] W. Du, R. Wang, and P. Ning, "An Efficient Scheme for Authenticating Public Keys in Sensor Networks," ACM, MobiHoc, 2005.

[3] L. Zhou and C. V. Ravishankar, "Dynamic Merkel Trees for verifying privileges in Sensor Networks," in *Proc. IEEE ICC 2006*.

[4] M. Jakobsson and S. Wetzel, "Efficient Attribute Authentication with Applications to Ad hoc Networks," ACM, VANET, 2004.

[5] V. Kondratieva and S-W Seo, "Optimized Hash Tree for Authentication in Sensor Networks," IEEE Communications Letters, Vol. 11, No. 2, Feb. 2007.

[6] ns-2 : Network Simulator, available at http://www.isi.edu/nsnam

[7] OpenSSL : Standard Cryptographic Library, available at http://www.openssl.org