センサセキュリティ技術

伊藤　隆*
米田　健**

Sensor Security Technology

Takashi Ito, Takeshi Yoneda

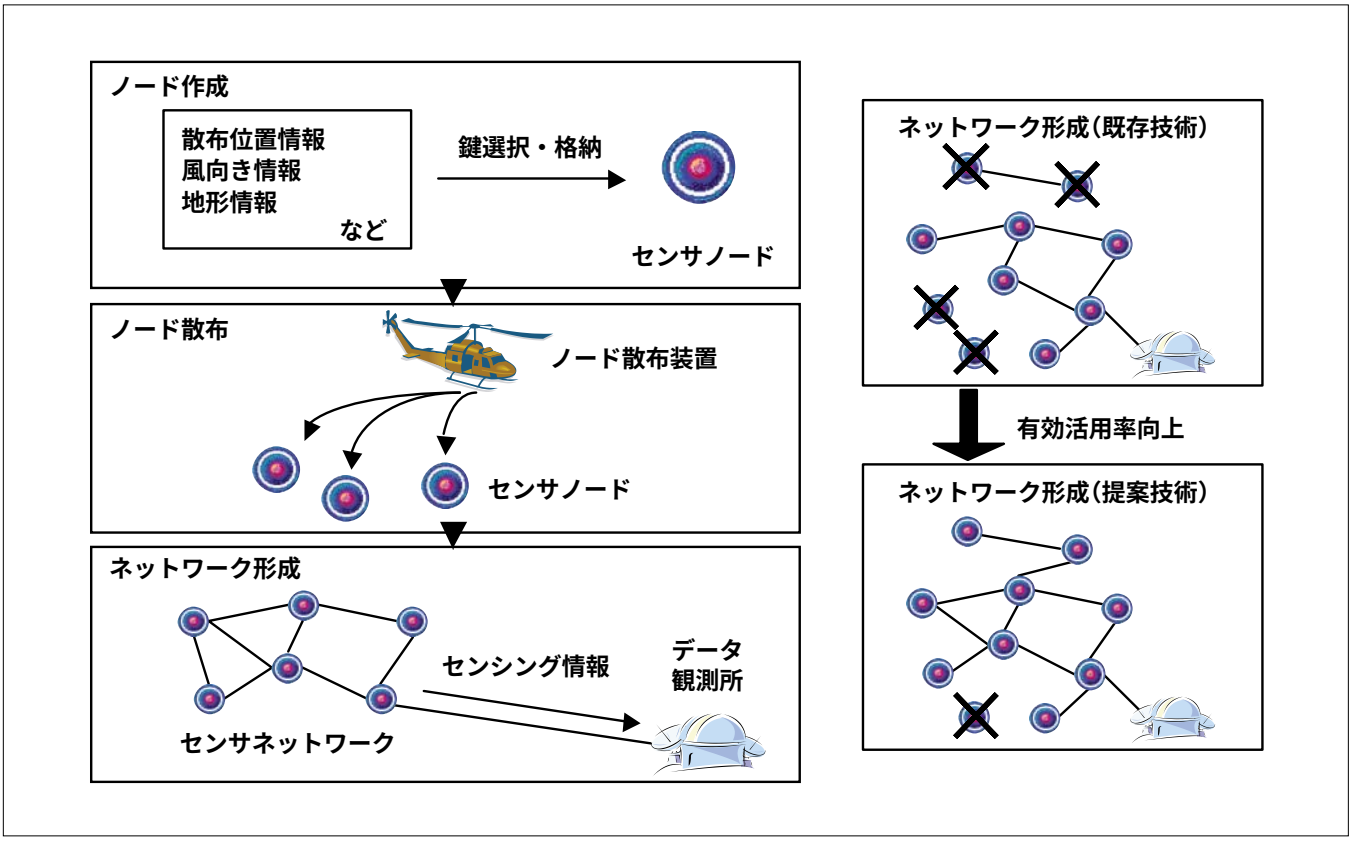
要　旨

センサネットワークは，大量のセンサノードから構成されるアドホックネットワークであり，ビル・工場管理，物流管理，環境情報の収集など，多方面への応用が期待されている。その中でも，ヘリコプターなどの移動体が広域を移動しながら大量のセンサノードを散布する“散布型センサネットワーク”は，迅速なネットワーク形成や，人手による設置が困難な場所でのネットワーク形成などが容易であるという好ましい性質を持つため，近年注目されている。

一般に，センサノード間の通信には無線が利用されるため，暗号化などのセキュリティ技術を用いた情報保護が必要不可欠である。このため，ノード間で安全に暗号鍵(かぎ)を共有する必要があるが，非力なCPU(Central Processing Unit)，小容量のメモリが用いられる散布型センサネットワークでの実現は容易ではない。

一つの解決策として，ランダムに選択した鍵を各ノードに格納し，確率的な鍵共有を可能とする“ランダム鍵格納方式”がある。また，この改良として，ノードを規則的に散布するという前提のもとで，鍵共有の成功確率を改善する方式が提案されている。しかしこれらの方式は，ノード散布手段に関する自由度が低く，散布手段によっては鍵共有の成功確率が大きく低下してしまうという問題があった。

我々の提案するランダム鍵格納方式では，散布における予想着地点の情報を鍵格納時に利用することで，任意の散布手段への適合を可能とする。提案方式について，鍵共有の成功確率を計算機実験によって評価した結果，散布の均一性を重視する散布手段のもとで，既存方式よりも40%高い成功確率を達成する結果が得られた。



散布型センサネットワーク

図左は散布型センサネットワークの形成手順を表したものである。散布位置などの事前情報を用いて選択した暗号鍵を各センサノードに格納し，これらノードをヘリコプターなどの移動体を用いて空中から散布する。図右は提案技術の利用による性能向上の様子を示したものである。安全に暗号通信を行えるノード対(線で結ばれたノード対)が増え，ネットワークから孤立するノード(×印のノード)を削減することができる。

*情報技術総合研究所　**同研究所(工博)